Monitor • Manage • Control

ContentKeeper Enterprise Administration Guide

For ContentKeeper Versions up to 121.04
Document Revision A
Date: 9th March 2004

Copyright © 2000, 2001, 2002, 2003, 2004 ContentKeeper Technologies

ContentKeeper®, Closed Loop Collaborative Filtering™ and *TrickleFeed*™ are trademarks of ContentKeeper Technologies. Copyright © 2000 - 2004, ContentKeeper Technologies, Canberra, Australia. All Rights Reserved.

Linux is a registered trademark of Linus Torvalds, Red Hat Linux is a registered trademark of Red Hat Inc.

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Intel® is a registered trademark of Intel Corporation and its subsidiaries in the United States and other countries.

eDirectory™, NDS and Novell® are trademarks of Novell Inc.

Microsoft®, Windows®, Windows NT and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this manual.

Document Author & Designer: Matthew R Richards
Introduction by David Williams

ContentKeeper Technologies
218 Northbourne Avenue
Braddon ACT 2612
Australia
PH +61-2-62614950
Fax +61-2-62579801
info@ContentKeeper.com
www.ContentKeeper.com

Table of Contents

Table of Contents **3**
Introduction **11**
Obtaining Technical Support 12
Obtaining Evaluation Software 12
Who should use this guide 13
Getting the most out of this guide 13
Document Conventions 13
Document Layout 14
An Introduction to the ContentKeeper Internet Content Filter 14
Chapter 1 QuickStart Guide **17**
Step 1. Prepare your ContentKeeper Appliance 19
Step 2. Configure the Management Port 20
Step 3. Perform the Initial Policy Configuration 21
Step 4. Connect the ContentKeeper Bridge Ports 22
Step 5. Monitor Reports and Tune Policies 24
Chapter 2 Building a ContentKeeper Appliance **27**
The ContentKeeper Appliance 28
The ContentKeeper SME Appliance 29
The ContentKeeper LE Appliance 30
Obtaining a ContentKeeper Appliance 32
Manually Building An Appliance 32
System Requirements 32
Minimum Hardware specifications 32
Supported Network Interface Cards (NICs) 33
Operating System 33
Optional High Availability Module 33
Obtaining Configuration Information 34
Hardware Setup 39
Ethernet Device Order 39
Rack Mounted Servers 39
Non-Rack Mount Servers 40
BIOS Setup 40
Power Management Features 40
Power Saving Features 40
System State After Power Failure 41
Plug and Play Feature 41
Device Boot Priority 41
BIOS Halt Feature 41
High Availability Module (H.A.M.) 42
Modes 42
Online Mode 42
Bypass Mode 42
High Availability Module Setup 43
Overview 43
Installing the High Availability Module 43
Identifying Ports on the H.A.M. 47
Connecting the Internet and Enterprise LAN ports 48

Identifying Cable Types....49
Completing H.A.M Configuration....50
Installing ContentKeeper....50
Using the ContentKeeper Auto Installer....50
The ContentKeeper Setup Program....51
Connecting the ContentKeeper Management Port....53
Accessing the ContentKeeper Setup Program from the ContentKeeper Console Screen....54
Accessing the ContentKeeper Setup Program from the Remote Serial Console....54
Remote Serial Console....55
Chapter 3 Deploying ContentKeeper....59
Introduction....60
Planning to Deploy ContentKeeper....61
Deployment Planning Guidelines....61
Deployment Planning Overview....61
Filtering of Local Network Segments....62
Filtering of Remote Network Segments....62
Filtering Proxy Server Traffic....63
ContentKeeper Bridge Port Location....64
ContentKeeper Management Port Location....67
Deploying ContentKeeper....68
Deployment Guidelines....68
Deployment Overview....69
Initial ContentKeeper Configuration....69
Making Space for the ContentKeeper Appliance....71
Deploying the ContentKeeper Appliance....71
Chapter 4 Administering ContentKeeper....73
ContentKeeper Administration Overview....74
What's involved in administering ContentKeeper?....74
The ContentKeeper Administration Life Cycle....75
ContentKeeper Filtering Explained....78
Policy Logic And Implementation Requirements....79
Closed Loop Collaborative Filtering....82
Live Filtering....83
Blocking Fundamentals....83
Blocking Types....83
Blocking States....87
Configuring ContentKeeper....90
Where to Start....90
Configuration Overview....91
Initial Configuration....91
Tuning Configuration....92
Configuration Tasks....92
Configuring the Management Port....92
The ContentKeeper Web Interface....93
Connecting ContentKeeper to the DataCenter....96
Configuring the HAM....97
Enabling Silent Mode....98
Excluded/Included IP Addresses....98

Configuring Bridge Device Settings....99
General Parameters....100
Configuring Logging....101
Configuring Username Resolution....101
Configuring Policies....102
An Overview of ContentKeeper Policies....102
Creating Custom Policies....103
Silent Mode....111
Configuring URL Reclassification....112
Configuring Live Filtering....112
Configuration Backups....113
ContentKeeper Reporting....114
Troubleshooting....115
Troubleshooting DataCenter Connectivity....115
Troubleshooting the H.A.M....118
Troubleshooting the Auto Installer....120
Rebuilding a ContentKeeper Appliance....121
How To Rebuild a ContentKeeper Appliance in 15 Minutes....121
Getting more help (technical support)....123
Chapter 5 Configuring ContentKeeper....124
Current Status Menu....125
Status Information....125
High Availability Module Status....126
Bridge Port Status....127
Bridge Traffic Status....128
DataCenter Connectivity Status....129
Current Internet Activity....129
Display Activity For Last....130
Display The Top....130
Current Blocking Activity....130
Display Activity For Last....131
Reconcile Usernames....131
Current Username Activity....132
Generate Report for Last Dropdown Box....132
Value Matching....132
Enter a Username or IP Address....133
Enter a Partial or Complete URL....133
Generate Report Button....133
View / Download Report Logs....134
View Report Logs Table....134
Report Log Settings....136
Dynamic Activity Viewer....137
Dynamic Activity Viewer Table....138
Internet Activity Viewer....138
Blocked Activity Viewers....139
Restart Menu....139
Restart ContentKeeper....140
Reboot ContentKeeper Appliance....140
Shutdown ContentKeeper Appliance....141
Administration Menu....141

Change Administration Password 142
View / Edit Reclassified URLS 142
Global Reclassified URLS 142
Category 143
Display Globally Reclassified URLs 143
Local URL Reclassifications 143
Display Local URL Reclassifications 144
Block/Unblock URLs In Control List 144
Using the Block/Unblock URLs in Control List Facility 145
Reclassification History 148
ContentKeeper Backups 148
Performing Backups 150
Download 150
Browse | Upload 150
Restore 151
Remove 151
Default-Setup-At-Installation 151
Miscellaneous Menu 152
Registration Details 152
Set/Adjust Date and Time 153
Update 154
Synchronize 154
Refresh 154
ContentKeeper Agent 154
Configuring ContentKeeper To Use The Agent 155
Installing The ContentKeeper Agent 156
Configuring The ContentKeeper Agent 158
Stopping And Restarting The Agent 159
Accessing the Agent Monitor 159
The Agent Log 160
Testing Connectivity 160
List Of Registered ContentKeeper Agents 161
Appliance Configuration Settings 162
Log Offloader 163
The Offloader Table 163
The Log Table 164
Zip Logs Before Transferring 165
View Status Log 165
Save and Test 166
Save and Execute Now 166
Turn off all Transfers 167
Blocking / Reporting Menu 167
Create & Edit Policies 168
Default Only Mode 168
Policy Cloning - Creating Custom Policies 169
Configuring Categories 169
Configuring File-Types 179
Configuring Custom URLs 181
Configuring Other Rules 184
Display Policies 185

Verify Policy 187
Category Aliases 190
Webalizer Reports 190
Webalizer Report Statistics 191
Report Types and Totals 192
Advanced Reporting Module 201
General Settings Menu 202
General Parameters 202
Port Numbers For Filtering 203
ContentKeeper Blocking 203
Excluded/Included IP Addresses 204
IP Address Table 204
Catch All Mode 205
Save And Verify 206
Example Excluded/Included IP Address Settings 206
Blockpage Customisation 207
Enabling Customised Blockpages 207
Configuring Customised Blockpages 207
Viewing Example Code 208
Testing Custom Blockpages 209
Username Resolution 210
Available Username Resolution Methods 210
None 210
IP Address 211
Proxy Header 216
Testing Username Resolution 219
Live Filtering Settings 222
Operational Settings Menu 225
Management Port Proxy Settings 225
Proxy Server Settings 225
Authentication Settings 226
Testing Connectivity 227
High Availability Module (H.A.M) 228
The H.A.M Settings Table 228
Managing the H.A.M 229
Configuring the H.A.M 231
URL Reclassification Settings 232
Configuring URL Reclassification 232
Reclassification Users 235
Bridge Device Settings 236
The Device Settings Table 236
Configuring Ethernet Device Settings 237
Selecting Bridge Device Settings 240
Authentication Menu 241
Site / Domain Authentication 241
Authenticate Against 242
Authentication Period 242
Clear Button 243
Local Users Database 243
Managing Local Users 244

Remote LDAP Databases 245
Departmental Reports Setup 248
Managing Departmental Reports User Accounts 248
Viewing Departmental Reports 250
LOCAL Groups 251
Managing LOCAL Groups 252
LDAP/eDirectory Groups 253
LDAP/eDirectory Users and Groups Setup Table 253
Enumerate Now 256
LDAP Log Results File 256
Chapter 6 Reference Section 257
Appendix A: NOTIFICATION OF COPYRIGHT AND LICENSE AGREEMENT 258
SOFTWARE LICENSE AGREEMENT - TERMS AND CONDITIONS 258
DEFINITIONS 259
1. Grant of License and Provision of Services 260
License 260
Payment 260
Evaluation 260
Blocking and Control Screens 260
General 260
2. Copyright Ownership and Confidentiality 261
3. Warranty 262
Appendix B: ContentKeeper Category Definitions 263
Introduction 263
Category 1: Adult Content 264
Category 2: News 264
Category 3: Job Search 264
Category 4: Gambling 265
Category 5: Travel / Tourism 265
Category 6: Shopping 265
Category 7: Entertainment 266
Category 8: Chatrooms 266
Category 9: Dating Sites 266
Category 10: Game Sites 267
Category 11: Investment Sites 267
Category 12: E-Banking 267
Category 13: Crime / Terrorism 268
Category 14: Personal Beliefs / Cults 268
Category 15: Politics 268
Category 16: Sports 269
Category 17: www-Email Sites 269
Category 18: Violence / Undesirable 269
Category 19: Malicious 270
Category 20: Search Sites 270
Category 21: Health Sites 270
Category 22: Clubs and Societies 271
Category 23: Music Downloads 271
Category 24: Business Oriented 271
Category 25: Government Blocking List 272

Category 26: Educational 272
Category 27: Advertising 272
Category 28: Drugs/Alcohol 273
Category 29: Computing/IT 273
Category 30: Swimsuit/Lingerie/Models 273
Appendix C: Glossary 274
Appendix D: ContentKeeper Technologies Global Office Location 278
Asia Pacific (Head Office) 278
Europe 278
Americas 278
Appendix E: High Availability Module Cable Specifications 279
Index 281

Introduction

Welcome to the ContentKeeper Enterprise Administration Guide. The purpose of the *Introduction* is to familiarise the reader with the content of, and the conventions used within the ContentKeeper Enterprise Administration Guide. This section also contains an introduction to the ContentKeeper product and information on obtaining technical support and evaluation software. Consider the introduction a reference section for the ContentKeeper Enterprise Administration Guide itself.

Obtaining Technical Support

Context Sensitive Help

The ContentKeeper web interface contains context sensitive help. Clicking on the *Help* hyperlink whenever it appears in the ContentKeeper web interface will access this help. The context sensitive help is based on this Administration Guide, and includes references to other online help sources as well as Administration Guide sections.

Technical Support

Technical support may be obtained from your local reseller, or from ContentKeeper Technologies Headquarters at the following address:

Mail: ContentKeeper Technologies
218 Northbourne Avenue
Braddon ACT 2612
Australia

Phone: +61 2 62614950

Fax: +61 2 62579801

Email: support@contentkeeper.com

Contact information for ContentKeeper Technologies Global Offices may be found at the end of this document under *Appendix E*.

Obtaining Evaluation Software

The ContentKeeper evaluation software consists of a full, unrestricted version of the ContentKeeper content filtering application and a 20-day trial subscription license. To upgrade to a 12 or 24-month subscription license, contact *ContentKeeper Technologies* or your local ContentKeeper reseller.

To obtain evaluation software, please browse to *www.contentkeeper.com* and select the *downloads* link. Fill in and submit the download registration form with your full contact details. The ContentKeeper software download instructions will be emailed to you.

Contact ContentKeeper Technologies to arrange a demonstration of the ContentKeeper appliance.

You may obtain the *ContentKeeper Auto Installer* ISO image by visiting the *Downloads* section of the ContentKeeper web site at www.contentkeeper.com and registering for an evaluation download.

Who should use this guide

This guide is designed for systems administrators and IT professionals who are responsible for installing, configuring and maintaining ContentKeeper. It is also designed for technical support personnel so that they may gain an understanding of components that are relevant to them.

Getting the most out of this guide

The ContentKeeper Enterprise Administration Guide, or the Administration Guide, is of a modular design. It consists of six chapters, all of which address different aspects of administering a ContentKeeper system. Within these chapters a heavy emphasis has been placed on cross-referencing to other sections of the Administration Guide.

The emphasis on cross-referencing removes the need to duplicate information within the Administration Guide. It also allows the reader to follow a path through the Administration Guide, to quickly identify the information that they need and avoid having to read entire sections.

To gain the most out of this Administration Guide, start by identifying the relevant section in the table of contents or the index, then read that section and follow any cross-references to other relevant sections.

Document Conventions

`All script and command-line instructions are in Courier New 14pt Bold type.`

Instructions for navigating to each menu feature within the ContentKeeper Web Interface will be displayed in inverse text at the start of each feature section.

For example (the instruction to access the *ContentKeeper Backups* menu):

Main Menu – Administration → ContentKeeper Backups

This would be interpreted in the following way. In the *main menu*, under the *administration section*, click on *ContentKeeper Backups*.

References to section titles within the Administration Guide or the *ContentKeeper Web Interface*, or to ContentKeeper product components will appear in *italic*.

Document Layout

The ContentKeeper Enterprise Administration Guide is divided into six chapters. The following is an overview of each chapter.

- **Introduction** – An introduction to the ContentKeeper Administration Guide.
- **Chapter 1 – QuickStart Guide** – This chapter enables administrators to deploy ContentKeeper quickly without having to read entire sections of the Administration Guide, or perhaps even fully understand why they are doing what they are doing.
- **Chapter 2 – Building a ContentKeeper Server** – This chapter details the various methods and procedures used, and requirements for installing ContentKeeper onto a server.
- **Chapter 3 – Planning to Deploy ContentKeeper** – This chapter consists of a detailed examination of the requirements of, and the procedures involved in deploying ContentKeeper into an organisation.
- **Chapter 4 – Administering ContentKeeper** – This chapter describes ContentKeeper management practices and troubleshooting procedures.
- **Chapter 5 – Configuring ContentKeeper** – This chapter consists of a detailed and technical description of each of ContentKeepers features and how they may be configured.
- **Chapter 6 – Reference Section** – This chapter contains information relevant to ContentKeeper but not suitable or too specialised for inclusion in other sections.

An Introduction to the ContentKeeper Internet Content Filter

Welcome to **ContentKeeper ®** the world's leading Internet Filtering technology.

We are delighted that you have decided to deploy a ContentKeeper Appliance in your network to provide filtered access for your Internet users.

In this Administration Guide you will find comprehensive instructions to help you set up your server hardware (the ContentKeeper Appliance), install the Linux Operating System and finally install and configure the ContentKeeper filtering software.

ContentKeeper has been designed from the outset to be easily installed in virtually any network and thereafter require the minimum of on-going administration.

The Appliance can be installed in networks with a variety of differing topologies and you will find several typical examples of these in the following pages. Simply stated, ContentKeeper should be installed between your

internal network and your Internet connection point, usually on the internal network side of your proxy and/or firewall. In this location ContentKeeper will be able to “see” the terminal devices on your organization’s network and identify the individual users for Internet activity reporting.

The Appliance presents itself as a transparent adaptive Ethernet bridge and is installed simply by patching it into your existing network. Installation can be normally accomplished without the necessity of re-configuring any of your other network devices. Being a bridge, ContentKeeper provides extremely fast filtering performance and is highly scaleable for use in high volume enterprise network environments.

Once installed, the Appliance establishes communication with the ContentKeeper DataCenter and automatically requests a registration key along with a download of the URL database that will be used in filtering your organization’s Internet access. Once downloaded, this database will be updated automatically every hour to ensure that it is current and can provide your organization with the most effective filtering possible.

The Appliance uses a combination of two filtering methodologies to ensure that your organization is provided with optimal filtering performance. These are; filtering based on the database of known Web Sites (filtering from the Control List described above) and Live Blocking. Live Blocking has been developed to enable ContentKeeper to identify and categorise new Web Sites which become active every few moments of every day and add them to its database in real-time.

ContentKeeper Technologies has designed the patent-pending **Closed Loop Collaborative Filtering ™** process. Using this technique, any newly identified web sites that are discovered by users connected through any ContentKeeper Appliance worldwide are sent back hourly to the ContentKeeper DataCenter for further analysis and verification prior to being added to the URL database. These newly discovered URLs are then made available in a download list, which is requested by Appliances in the field as part of the automatic hourly update.

We at ContentKeeper Technologies welcome you as a ContentKeeper user and assure you of our on-going commitment to provide you with the best Internet Filtering Technology available.

Note: For more general and conceptual information on ContentKeeper Internet content filtering, refer to the ContentKeeper web site at www.contentkeeper.com.

Chapter 1

QuickStart Guide

Chapter 1, the *QuickStart Guide*, has the purpose of enabling users to deploy ContentKeeper quickly without having to read entire sections of the Administration Guide. The *QuickStart Guide* is a short section that is presented in a simple fashion and contains mainly overviews of tasks with comprehensive cross-referencing to other relevant sections within the Administration Guide.

Welcome to the *QuickStart Guide,* the purpose of which is to get your ContentKeeper up and running as quickly and with as little effort as possible.

The *QuickStart Guide* assumes the reader has no prior knowledge of ContentKeeper, and as such it contains only the most basic information, with cross-references to supplemental material. All underlined links may be found in either the Table of Contents or the index.

You will need a hardware platform to be your ContentKeeper Appliance. ContentKeeper Technologies supplies two dedicated appliances, one for small to medium enterprise and one for large enterprise.

Note: Refer to The ContentKeeper Appliance section in Chapter 2 for information on obtaining or building a dedicated ContentKeeper appliance.

The *QuickStart Guide* assumes that the reader already has a pre-built ContentKeeper appliance.

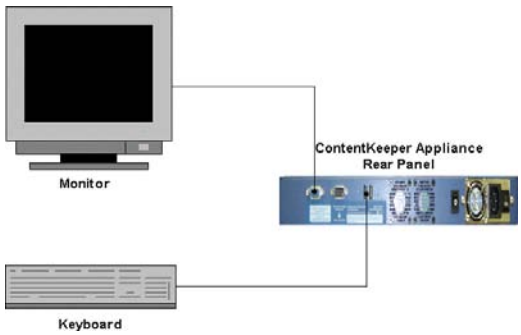
Note: For an introduction to ContentKeeper refer to An Introduction to the ContentKeeper Internet Content Filter and to the ContentKeeper web site at www.contentkeeper.com.

Lets get started . . .

Step 1. Prepare your ContentKeeper Appliance

Unpack the ContentKeeper appliance and then attach either a monitor and keyboard (*Video Console*) or a *Remote Serial Console*.

To attach a *Video Console* to a ContentKeeper appliance, first plug a standard monitor into the DB15 video connector on the rear panel of the appliance. Next, plug a USB keyboard into one of the USB connectors on the rear panel of the appliance.



Note: Refer to the Remote Serial Console section in Chapter 2 for instructions on using the *Remote Serial Console*.

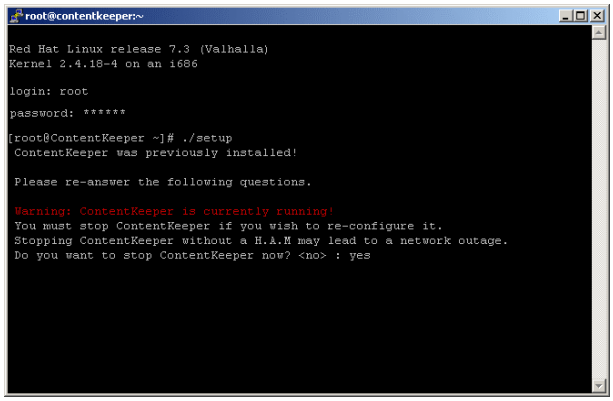
Print out and complete the *Administrative Details* and *Configuration Details* lists under the Obtaining Configuration Information section in Chapter 2.

Configuration Details	Value
Management Port IP Address This is the only IP address that ContentKeeper needs. This IP address will be used to access the *ContentKeeper Web Interface* from your network, and for downloading hourly *Control List* updates. It is usually a private IP address behind your firewall.	
Management Port Host Name The name of the ContentKeeper server (not the fully qualified domain name, which will be specified later).	
Management Port Netmask This is the netmask for the *Management Port* IP address.	
Proxy Server IP Address This may be necessary if your network devices need to use a caching proxy server to access the Internet, as ContentKeeper may also need to use these settings to access the *ContentKeeper DataCenter* for its hourly *Control List* updates.	
Proxy Server Port Number This is the port number that the proxy server is listening on (eg: port 8080, 3128 etc).	
Proxy Server Authentication (Y/N) Does the proxy server that your network devices (Eg. Internet browsers) use to connect to the Internet require authentication?	
Is Proxy Bypass Possible (Y/N) This may be necessary if the proxy server requires authentication, as the ContentKeeper *Management Port* can only negotiate proxy server authentication when the Basic authentication scheme is supported. Is it possible to configure a rule within your proxy server to allow the ContentKeeper *Management Port* to bypass authentication?	

The information that you provide will be used in the next step and will also be very useful as a reference when performing the initial ContentKeeper configuration.

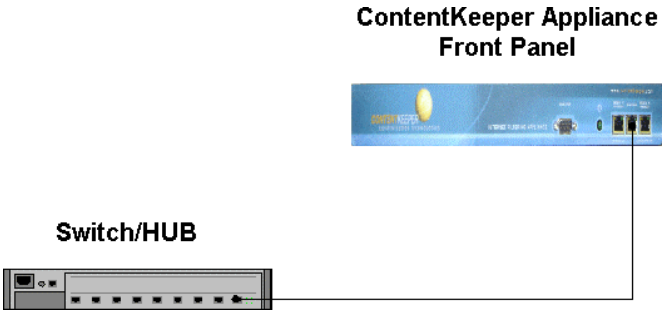
Step 2. Configure the Management Port

Logon to the appliance and use the ContentKeeper *Setup Program* to configure the IP address settings of the *Management Port*. Just type **`setup`** at the command prompt. Answer all of the questions and answer *Yes* to the final question to reboot the appliance.


root@contentkeeper:~
Red Hat Linux release 7.3 (Valhalla)
Kernel 2.4.18-4 on an i686
login: root
password: ******
[root@ContentKeeper ~]# ./setup
ContentKeeper was previously installed!
Please re-answer the following questions.
Warning: ContentKeeper is currently running!
You must stop ContentKeeper if you wish to re-configure it.
Stopping ContentKeeper without a H.A.M may lead to a network outage.
Do you want to stop ContentKeeper now? <no> : yes

Note: Refer to The ContentKeeper Setup Program section in Chapter 2 for instructions on using the ContentKeeper *Setup Program*.

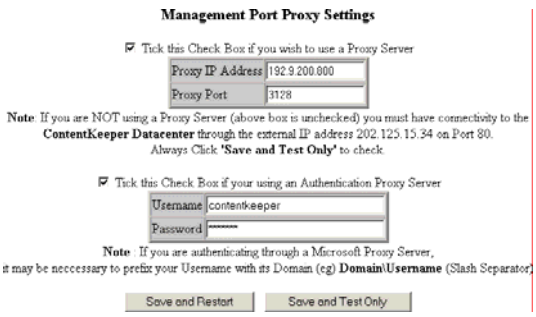
Use a straight-thru cable to attach the ContentKeeper *Management Port* to a Switch or Hub on your network and allow ContentKeeper to register with the *ContentKeeper DataCenter*. ContentKeeper must have Internet connectivity.



The Management Port is the middle Ethernet port on the ContentKeeper *SME Appliance* and the bottom right port on the ContentKeeper *LE Appliance*. All ports are labelled.

Note: Refer to the ContentKeeper Management Port Location section in Chapter 3 for more information about connecting the ContentKeeper *Management Port*.

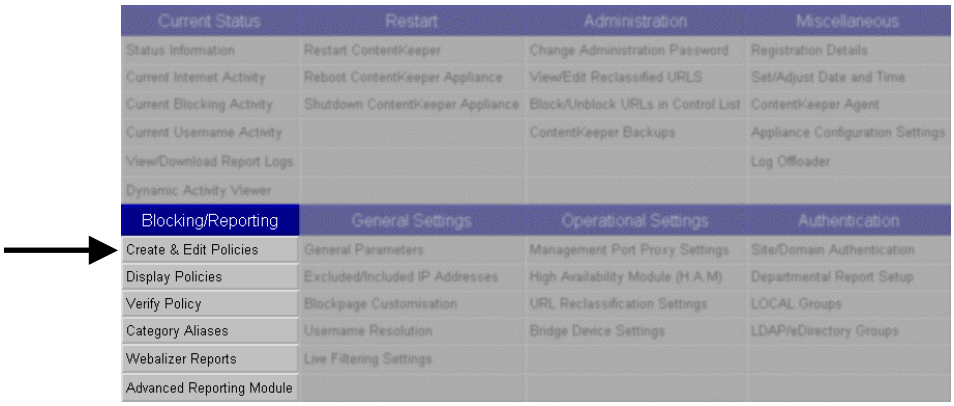
If your organisation employs an authenticating proxy server, you may need to access the *ContentKeeper Web Interface* to configure authentication settings in the *Management Port Proxy Settings* menu.


Management Port Proxy Settings
Tick this Check Box if you wish to use a Proxy Server
Proxy IP Address 192.9.200.800
Proxy Port 3128
Note: If you are NOT using a Proxy Server (above box is unchecked) you must have connectivity to the ContentKeeper Datacenter through the external IP address 202.125.15.34 on Port 80.
Always Click 'Save and Test Only' to check.
Tick this Check Box if your using an Authentication Proxy Server
Username contentkeeper
Password ••••••••
Note: If you are authenticating through a Microsoft Proxy Server,
it may be neccessary to prefix your Username with its Domain (eg) Domain\Username (Slash Separator)
Save and Restart
Save and Test Only

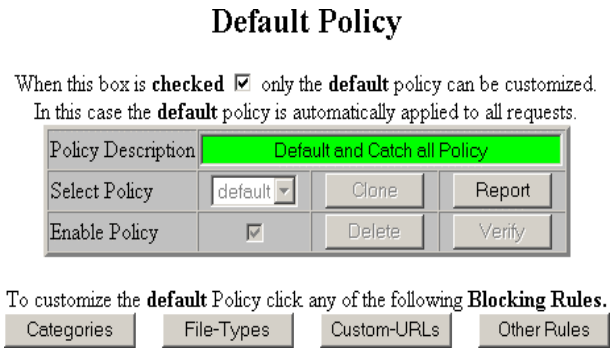
Note: Refer to the Management Port Proxy Settings section in Chapter 5 for information on configuring *Management Port* proxy authentication settings.

Step 3. Perform the Initial Policy Configuration

Browse to the *ContentKeeper Web Interface*, select *Create & Edit Policies* from the *Blocking/Reporting* menu and then configure *Categories*, *File Types* and *Custom URLs* for the *Default* policy.



We recommend starting with a simple configuration and then build upon it. This allows easy assessment of the effects of configuring various policy components.

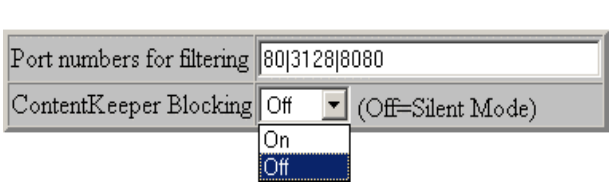


Note: Refer to the Categories, File Types and Custom URLs sections under the Create & Edit Policies section in Chapter 5 for information on configuring policy components.

The factory-set *Default Policy* configuration is a typical workplace policy and is a good starting point that can be built upon to form comprehensive filtering policies tailored to your specific environment.

Note: Refer to the Configuring ContentKeeper section in Chapter 4 for general information on configuring ContentKeeper.

Consider using ContentKeeper in *Silent Mode* during the first stages of its implementation. This will allow you to determine if the policy settings are too restrictive or not restrictive enough without Internet users being aware that policy adjustments are taking place. The *Default Policy* may then be fine tuned without affecting Internet access.



Step 4. Connect the ContentKeeper Bridge Ports

ContentKeeper is a transparent adaptive Ethernet bridge able to pass any type of Ethernet traffic, and specifically designed to filter HTTP traffic, including proxy encapsulated and WCCP-GRE encapsulated traffic.

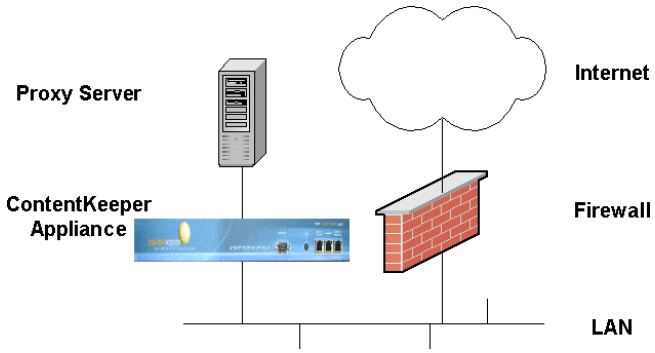
Deploy ContentKeeper by connecting the *Bridge Ports* to your network. To guide you through the process of connecting the *Bridge Ports* to your network, the two most common ContentKeeper deployment scenarios are shown below.

Note: The *Quickstart Guide* does not include information about connecting the *High Availability Module*, which requires different cable types to ContentKeeper when connected to a network. Refer to the High Availability Module (H.A.M) section in Chapter 2 for information about connecting and configuring the *High Availability Module*.

Deployment Scenario One

The first deployment scenario listed here is also the most common. In this scenario ContentKeeper is deployed to a network where a proxy server is being used.

ContentKeeper is placed between the users and the Internet. In this scenario ContentKeeper is located between the users and the proxy server, allowing ContentKeeper to see where each request is coming from. When an authenticating proxy server is being used ContentKeeper can also see who made each request.



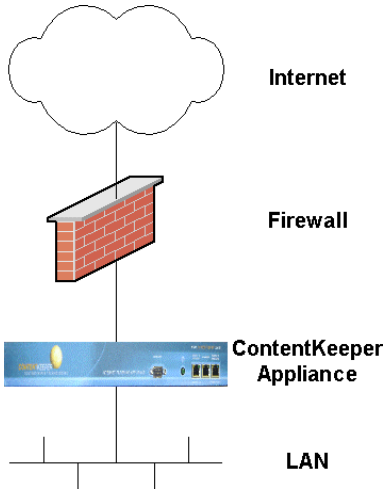
The ContentKeeper *Bridge Ports* are network interfaces just like those on any normal workstation. For this reason different cables must be used when connecting the *Bridge Ports* to different network devices.

In this scenario one of the *Bridge Ports* is connected to the proxy server with a Cross-Over cable, and the other *Bridge Port* is connected to the LAN (i.e. a Hub or Switch) with a Straight-Thru cable.

Important! When ContentKeeper is deployed in this scenario, always add the IP address of the proxy server to the ContentKeeper *Excluded/Included IP Addresses* list. This prevents ContentKeeper from filtering URL requests made by the proxy server, as ContentKeeper is designed to block inappropriate requests on their way to the proxy server from the users.

Deployment Scenario Two

The second deployment scenario listed here involves deploying ContentKeeper to a network where no proxy server is being used.



ContentKeeper is placed between the users and the Internet. In this scenario ContentKeeper is located between the users and the Internet gateway (Firewall). This usually allows ContentKeeper to see where each request is coming from.

The ContentKeeper *Bridge Ports* are network interfaces just like those on any normal workstation. For this reason different cables must be used when connecting the *Bridge Ports* to different network devices.

In this scenario one of the *Bridge Ports* is connected to the firewall server with a Cross-Over cable, and the other *Bridge Port* is connected to the LAN (i.e. a Hub or Switch) with a Straight-Thru cable.

Note: Refer to the ContentKeeper Bridge Port Location section in Chapter 3 for more information about connecting the ContentKeeper *Bridge Ports*.

Check Your Internet Connectivity

Once you have connected the *Bridge Ports*, ensure that ContentKeeper is bridging network traffic by browsing to the *Status Information* menu in the *ContentKeeper Web Interface*. Refresh the browser window to see changes in traffic throughput.

Note: The numbers next to *RX bytes (ethx)* and *RX packets (ethx)* indicate the amount of data and number of packets being received by the *Bridge Ports*, and hence the amount of network traffic traversing the *ContentKeeper Bridge*.

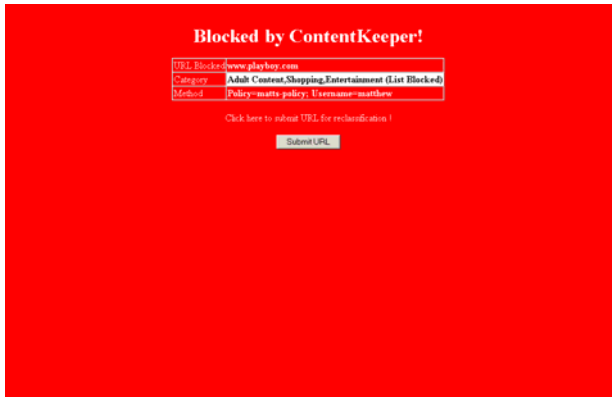
At this point you should also test your connection to the Internet by browsing from a separate workstation to the Internet. We recommend that you browse to a well-known web site so that you may verify that Internet access if performing normally.

Step 5. Monitor Reports and Tune Policies

Once ContentKeeper has been deployed you should verify that it is blocking and reporting as expected. Start by browsing from a filtered workstation to a URL that you know will be blocked.

Note: Select *Create & Edit Policies* from the *Blocking/Reporting* menu in the *Web Interface* and click the *Categories* button to see which categories you set to block in *Step 3*, and hence which types of URL will be blocked.

You should receive a *blockpage* similar to the one on the right when you request the URL. If you have configured *Blockpage Customisation* the *blockpage* may appear differently.



Remember, if you have deployed ContentKeeper in *Silent Mode* you will not be blocked, instead ContentKeeper will report your request in the *Current Blocking Activity* report and in the Dynamic Internet Activity viewer window.

Check the Current Internet Activity Report

To verify that ContentKeeper is reporting Internet activity correctly, select *Current Internet Activity* from the *Current Status* menu in the *Web Interface* and click the *Display* button. You should see URLs and IP addresses / Usernames generated by users browsing the Internet.

Note: Refer to the Current Internet Activity section in Chapter 5 for further information.

Check the Current Blocking Activity Report

To verify that ContentKeeper is reporting Blocked activity correctly, select *Current Blocking Activity* from the *Current Status* menu in the *Web Interface* and click the *Display* button. You should see URLs, IP addresses and blocking details generated by users browsing to blocked sites.

Note: The *Current Blocking Activity* menu is where ContentKeeper will report blocking activity if you have enabled *Silent Mode*. Refer to the Current Blocking Activity section in Chapter 5 for information.

Now that ContentKeeper has been deployed, you may wish to tune the *Default Policy* and/or create *Custom Policies*. Continue to monitor the *Current Internet Activity* and *Current Blocking Activity* reports to see how your Default policy has affected Internet access for your organisation, and to gain an insight into how you should configure *Custom Policies* if you choose to do so. Remember to enable a new policy after you create it.

You may also wish to examine the *Current Username Activity* report and the *Dynamic Activity Viewer*.

Note: Refer to the Current Username Activity section in Chapter 5 for information on using the *Current Username Activity* report. Refer to the Dynamic Activity Viewer section in Chapter 5 for information on using the *Dynamic Activity Viewer*.

Read the Configuring ContentKeeper section in Chapter 4 for more general information about configuring ContentKeeper.

Read the Configuring Policies section in Chapter 4 for a discussion on creating *Custom Policies* including an overview of the procedure.

Read the ContentKeeper Reporting section in Chapter 4 for a discussion of the available reporting methods.

Congratulations!
You have successfully deployed ContentKeeper.

Chapter 2

Building a ContentKeeper Appliance

Chapter 2, *Building a ContentKeeper Server*, details the various methods and procedures used when installing ContentKeeper onto a server. It contains information on system requirements and installation media. This section also contains information on installing the *High Availability Module* as well as operating environment considerations. This section will contain cross-referencing to other relevant sections within the Administration Guide.

The ContentKeeper Appliance

The *ContentKeeper Appliance* is a fully self-contained Internet content filtering hardware solution provided by ContentKeeper Technologies. The *ContentKeeper Appliance* is available in two models, the small enterprise model (SME) suitable for small to medium, Fast Ethernet (10/100 Mbps) networks, and the large enterprise model (LE) suitable for medium to large, Fast Ethernet (10/100 Mbps) or Gigabit (1000 Mbps) networks.

Like all ContentKeeper deployments, the *ContentKeeper Appliance* requires no operating software maintenance, and all software updates and URL Database updates are completely automated.

Each *ContentKeeper Appliance* package contains the following:

- ContentKeeper Appliance
- ContentKeeper Auto Installer CD
    - ContentKeeper Enterprise Administration Guide
    - ContentKeeper Multimedia Presentations
    - ContentKeeper Product Brochures
- Power Lead
- Serial Cable
- Rack Mount Kit
- Little Rubber Feet (LRF) for non-rack mount deployment

Refer to the following table when choosing the right appliance for your network.

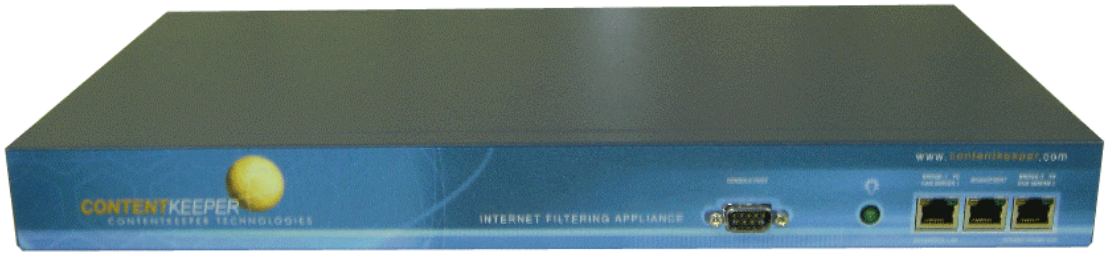
Appliance	Max. Users	Max. Bandwidth	H.A.M Support (1)	Fibre Optic Support (2)
SME	2,500	100 Mbps	√	
LE	50,000	1000 Mbps (Gigabit)	√	√

(1) The *ContentKeeper High Availability Module* may be purchased as an optional extra for the *ContentKeeper Appliance*.

(2) Fibre optic network interface modules may be purchased as an optional extra for the *ContentKeeper LE Appliance*.

The ContentKeeper SME Appliance

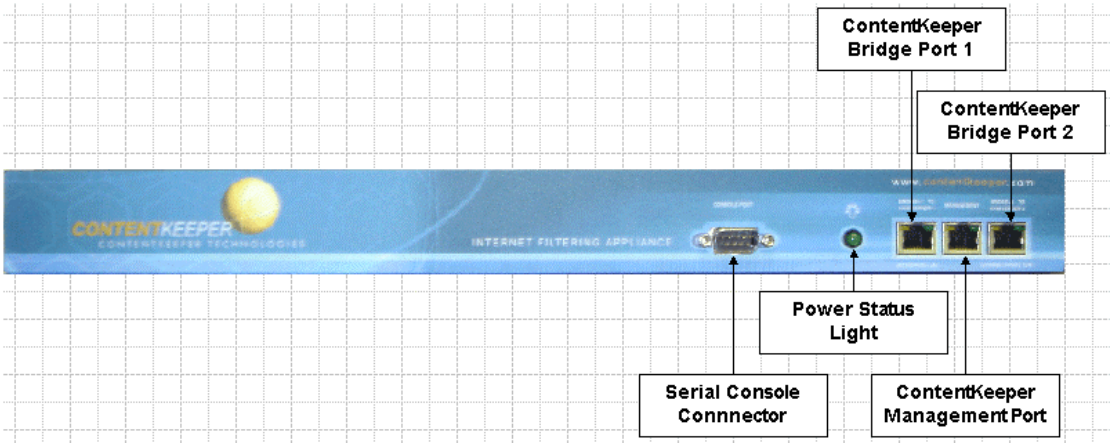
The *ContentKeeper SME Appliance* has been designed for the small to medium enterprise. The *SME Appliance* supports sites from twenty-five users up to approximately two and a half thousand users.



The *ContentKeeper SME Appliance* also supports UTP Ethernet networks up to a maximum bandwidth of 100 Mbps.

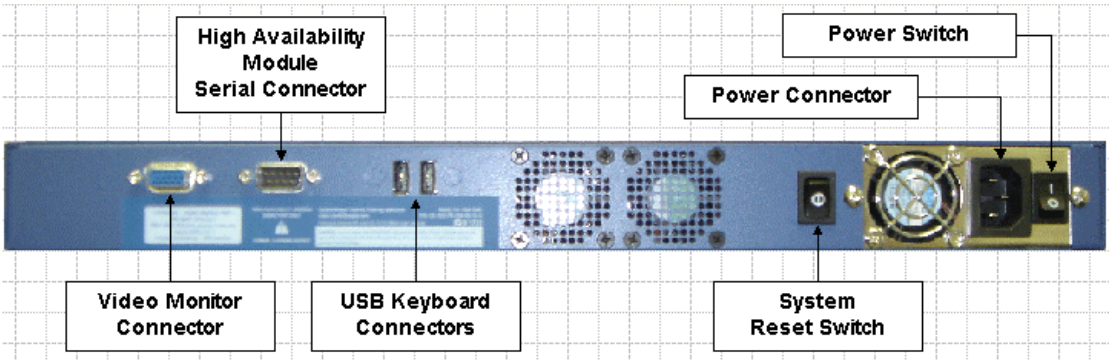
SME Appliance Front Panel

The *ContentKeeper SME Appliance* front panel provides the *Bridge Ports* and *Management Port*, as well as a serial connector for *Remote Serial Console* attachment and a power status light.



SME Appliance Rear Panel

The *ContentKeeper SME Appliance* rear panel provides a serial connector for *H.A.M* attachment, a video connector for monitor attachment, USB connectors for keyboard attachment, a reset switch, a power switch and a power connector.



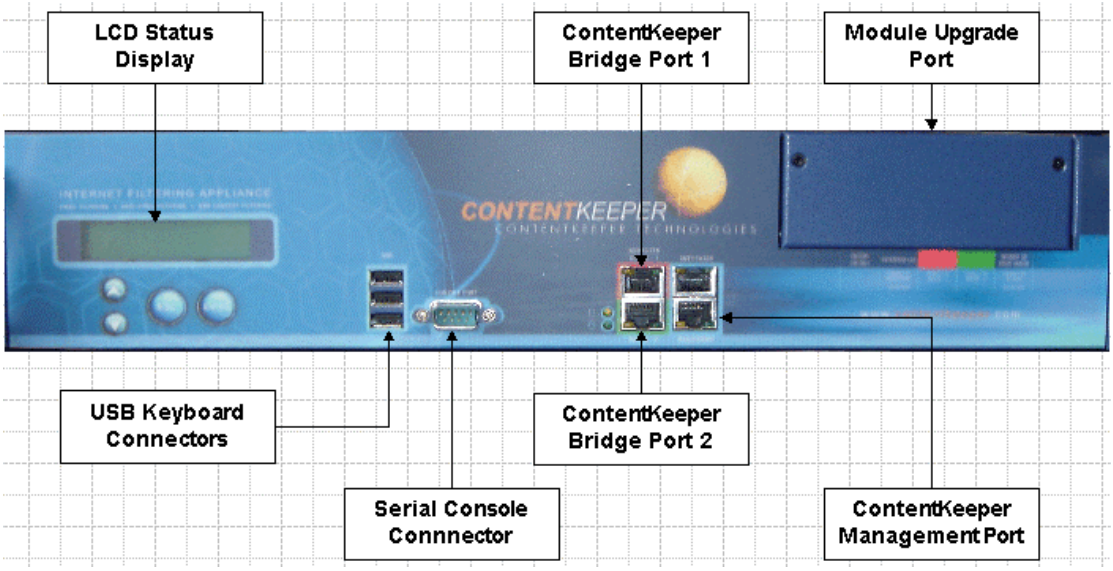
The ContentKeeper LE Appliance

The *ContentKeeper LE Appliance* has been designed for the medium to large enterprise. The *LE Appliance* supports sites from two thousand users up to approximately fifty thousand users.

The *ContentKeeper LE Appliance* also supports UTP and Fibre Optic Ethernet networks up to a maximum bandwidth of 1000 Mbps (Gigabit).

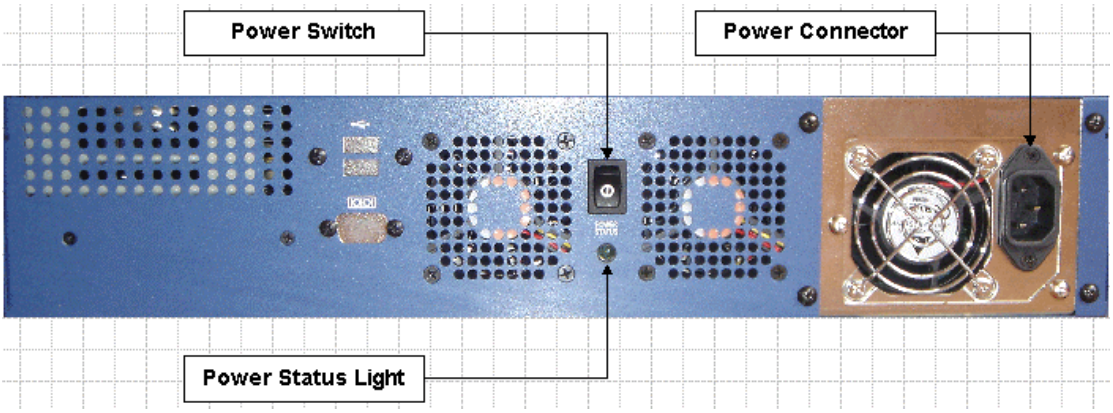
LE Appliance Front Panel

The *ContentKeeper LE Appliance* front panel provides the *Bridge Ports* and *Management Port*, a module upgrade port for the optional *High Availability Module* and *Fibre Optic Network Interface Modules*, an LCD display for appliance status, USB connectors for keyboard attachment, as well as a serial connector for *Remote Serial Console* attachment.



LE Appliance Read Panel

The *ContentKeeper LE Appliance* rear panel provides a power switch and a power connector.



Obtaining a ContentKeeper Appliance

Note: Refer to the Obtaining Evaluation Software section in the Introduction for more information on evaluating or purchasing a ContentKeeper appliance.

Manually Building An Appliance

ContentKeeper is not limited to operating on the SME or LE appliances; it will also operate on any Intel based hardware that meets the minimum system requirements. You can supply your own hardware and use the *ContentKeeper Auto Installer* to manually build an appliance.

The remainder of this chapter is dedicated to the task of building a ContentKeeper appliance.

Note: Refer to the Obtaining Evaluation Software section in the Introduction for more information on obtaining a ContentKeeper *SME* or *LE Appliance*, and the *ContentKeeper Auto Installer*.

System Requirements

The following sections detail the system requirements for a ContentKeeper appliance. The system requirements listed here are for an environment with a maximum of approximately two and a half thousand users. To build a ContentKeeper appliance for a larger environment, double the CPU, Memory and Storage requirements.

Minimum Hardware specifications

Dedicated Intel based PC, 1GHz CPU, 512MB RAM, 10GB HDD,
3 x 10/100Mbit/s or Gigabit Ethernet Cards UTP, Keyboard.

Important: The *ContentKeeper Auto Installer* will automatically configure the system swap space to approximately double the amount of system RAM. ContentKeeper must have a minimum of 750 MB of combined RAM and swap to operate. This means that a ContentKeeper appliance must have a minimum of 256 MB RAM in order for ContentKeeper to operate.

Note: A ContentKeeper appliance built with less than the recommended amount of RAM is only suitable for evaluation purposes.

Supported Network Interface Cards (NICs)

(At time of publication)

- Intel Pro™ 10/100 Server Adapters (This includes most NICs based on the Intel 82557 or 82559 chipset)
- Intel Pro™ 1000 Server Adapters (This includes dual port adapters)

The Intel Pro™ chipset is widely supported throughout the Linux community, and is an industry standard architecture for PCI Ethernet cards. It is supported for use with most versions of Linux and all Intel based hardware.

The Intel Pro™ chipset was the first chipset to be fully supported for use with ContentKeeper. When ContentKeeper is installed on a system that contains three Intel Pro™ NICs, new features becomes available in the *Bridge Device Settings* menu that enable configuration of the bandwidth (speed) and duplex of the installed Ethernet cards.

Note: Refer to the Bridge Device Settings section in Chapter 5 for more information.

The following list of Hardware is **incompatible** with ContentKeeper:

- NetGear Ethernet Devices

Operating System

The following operating systems are compatible with ContentKeeper. *ContentKeeper Technologies* will not be able to provide support nor guarantee that ContentKeeper will operate on any other operating system.

- Red Hat Linux v7.2
- Red Hat Linux v7.3

Optional High Availability Module

The *ContentKeeper High Availability Module (H.A.M)* is an optional extra that may be used with any ContentKeeper appliance, pre-built or otherwise. The *H.A.M* is available from your local ContentKeeper Channel Partner, or from ContentKeeper Technologies.

Note: Refer to the Obtaining Evaluation Software section in the Introduction for more information on obtaining a *H.A.M*. Refer to the High Availability Module (H.A.M) section in this chapter for more information on installing the *H.A.M*.

Obtaining Configuration Information

Some network and administrative information is required to install ContentKeeper. All of the necessary information can be obtained by completing the lists on the following pages.

It is recommended that the following lists be completed before ContentKeeper is installed. The information obtained by completing the lists will also be very useful as a reference when performing the initial ContentKeeper configuration.

Administrative Details	Value
Company Name	
Technical Contact	
Billing Contact	
Address Line 1	
Address Line 2	
City	
State	
Zipcode/Postcode	
Telephone Country Code	
Telephone Area Code	
Telephone Number	
Fax Number	
Email Address	

Configuration Details	Value
Management Port IP Address This is the only IP address that ContentKeeper needs. This IP address will be used to access the *ContentKeeper Web Interface* from your network, and for downloading hourly *Control List* updates. It is usually a private IP address behind your firewall.	
Management Port Host Name The name of the ContentKeeper server (not the fully qualified domain name, which will be specified later).	
Management Port Netmask This is the netmask for the *Management Port* IP address.	
Proxy Server IP Address This may be necessary if your network devices need to use a caching proxy server to access the Internet, as ContentKeeper may also need to use these settings to access the *ContentKeeper DataCenter* for its hourly *Control List* updates.	
Proxy Server Port Number This is the port number that the proxy server is listening on (eg: port 8080, 3128 etc).	
Proxy Server Authentication (Y/N) Does the proxy server that your network devices (Eg. Internet browsers) use to connect to the Internet require authentication?	
Is Proxy Bypass Possible (Y/N) This may be necessary if the proxy server requires authentication, as the ContentKeeper *Management Port* can only negotiate proxy server authentication when the Basic authentication scheme is supported. Is it possible to configure a rule within your proxy server to allow the ContentKeeper *Management Port* to bypass authentication?	

Configuration Details	Value
Does the Gateway Device Pass TCP Port 80 Traffic (Y/N) If your network employs an authenticating proxy server that cannot be bypassed by the *Management Port* then it may be necessary to explicitly bypass the proxy server. For this to be successful, the gateway device (eg. a firewall) must pass outbound TCP traffic on port 80 (HTTP Protocol) from the ContentKeeper *Management Port*.	
DNS IP Address If your network has a DNS server, then this is its IP address.	
Domain Suffix This is the primary domain suffix of the domain to which the *Management Port* is connected to, eg. The domain suffix for a system located at ContentKeeper Technologies is <contentkeeper.com>.	
Firewall Internal IP Address If there is a firewall protecting your network from the Internet, then that Firewall's configuration information may be needed when configuring ContentKeeper.	
Firewall Caching Proxy Server Port Number Is there a caching proxy server running on the firewall that is not the proxy server that your workstations use to connect to the Internet.	
Directory Service Does the network use a directory service? For example Windows NT/2000 use Active Directory, Novell uses NDS.	
Fibre-Optic Network Connectivity Is there Fibre-Optic cable in the internal network, i.e. between the proxy server and the gateway, or between the switch and the proxy server? The type of network cabling being attached to the *ContentKeeper Bridge Ports* will determine the hardware used within the ContentKeeper appliance.	

Configuration Details	Value
Network Bandwidth What is the maximum bandwidth available on your network for Internet access, e.g. usually the speed of your WAN link to the Internet?	

Hardware Setup

Ensure that there are three NICs installed in the ContentKeeper server. ContentKeeper Technologies does not support systems built with less than three NICs. All NICs should be PCI cards, not ISA. Systems containing ISA cards are not supported.

Note: It is recommended that the three NICs be of the same model. Refer to the System Requirements section in this chapter for information on which NICs to use.

Ethernet Device Order

An understanding of Linux Ethernet device-name assignments and the order of the Ethernet devices within your system will be necessary when configuring ContentKeeper.

Under Linux, Ethernet devices are given the label of "ethN" where "N" is the device number. The device number is determined by Linux at boot and reflects the order in which Linux accesses the device from the PCI bus.

Usually the order of access starts with any onboard Ethernet devices and then goes from the PCI slot closest to the CPU to the PCI slot furthest from the CPU.

You will need this information when using the ContentKeeper *Setup Program* to configure which Ethernet interfaces will be the Bridge Ports and which will be the Management Port.

Note: Refer to The ContentKeeper Setup Program section in this chapter for information.

Rack Mounted Servers

In rack mounted systems there are usually two NICs embedded into the system board. These two NICs should become the bridge ports. The reason for this is that there will be no difference in the time that the system takes to access either NIC and therefore this configuration will result in a more efficient bridge (through guaranteed hardware symmetry).

In some servers one embedded NIC is a gigabit and the other a fast Ethernet (i.e. 10/100 mbps) NIC. In servers with this configuration, one of the embedded NICs should be configured as the Management Port, while an additional two NIC should be installed and configured as the Bridge Ports.

Non-Rack Mount Servers

In non-rack mount systems, the middle card should become the management port, while the outer two cards become the bridge ports. The middle card will usually be defined as eth1 under Linux. This arrangement is recommended as the management port is easily identified as the middle PCI card with a bridge card on either side.

There should be no difference in the time that the system takes to access any NIC.

BIOS Setup

This section contains general guidelines for configuring BIOS on a ContentKeeper appliance.

ContentKeeper Technologies recommends a specific configuration for several standard BIOS features. Each feature is listed below with configuration details. For any BIOS settings that are not listed here, use values that are appropriate to the system on which the BIOS is installed. The BIOS Features to be specifically configured for ContentKeeper are:

- Power Management Features
- Plug and Play Feature
- Device Boot Priority
- BIOS Halt Feature

To configure BIOS, boot the server and press the appropriate key when prompted to enter BIOS setup (This is usually the *Delete* key).

Power Management Features

BIOS power management features can usually be accessed from a *Power Management* or similarly titled menu.

Power Saving Features

All power saving features should be disabled, including Advanced Power Management, Suspend, and Wake-On-LAN. This is to prevent the ContentKeeper appliance from automatically powering down at any time.

System State After Power Failure

The server should be configured to power **on** after a power failure to prevent the need for a manual reset after a power outage. This configuration option is often labelled differently for different BIOS manufacturers. Some examples are “System after AC Back” and “State after power failure”.

Plug and Play Feature

This feature can usually be accessed from a *PNP/PCI Management Setup* or similarly titled menu. The *Plug and Play Operating System Installed* option should be *Disabled* or set to *No*.

Device Boot Priority

These features can usually be accessed from a *Boot*, *Advanced* or similarly titled menu.

For secure and uninterrupted operation the appliance should only be able to boot from the storage device on which ContentKeeper is installed. This will probably be one of the following:

- HDD
- HDD-0
- SCSI
- R.A.I.D. Array

Usually there is a minimum of three entries to configure under boot device priority. If it is possible, it is recommended that only the first hard drive be configured and that any further entries are set to *Disabled*.

BIOS Halt Feature

This feature can usually be accessed from a *Standard CMOS Setup* or similar menu.

Using this feature, the system BIOS should be set to halt on no errors. This is to enable the system to boot even if there is no keyboard or monitor attached.

Save and exit from BIOS configuration!

High Availability Module (H.A.M.)

PLEASE READ THIS SECTION CAREFULLY – It is essential that each *H.A.M* port be correctly identified and that the appropriate cables are used to ensure proper operation of the *H.A.M*.

The ContentKeeper optional *High Availability Module* is an electromechanical Ethernet Bypass Switch. The *H.A.M* is used to help prevent a network outage in the unlikely event of a hardware or software failure on the ContentKeeper appliance. This functionality is achieved by the *H.A.M* monitoring Ethernet Link Status as well as a heartbeat from the ContentKeeper appliance.

There are two types of *High Availability Module*. They are an external self-contained module and an Internal PCI card module. Both operate identically. Additionally, both types of *High Availability Module* are available in a Fast Ethernet model (10/100 Mbps) and a Gigabit model (1000 Mbps).

Modes

The H.A.M. has two modes, *Online* and *Bypass*.

Online Mode

In *Online* mode the *Internet Port* is connected to *Bridge Port 1* and the *Enterprise LAN Port* is connected to *Bridge Port 2*. The H.A.M. will remain in this mode while there is a link heartbeat coming from both the bridge ports, and the serial interface port (these are known as the *Online* conditions).

Bypass Mode

In *Bypass* mode the *Internet Port* is connected directly to the *Enterprise LAN Port*, bypassing the ContentKeeper appliance.

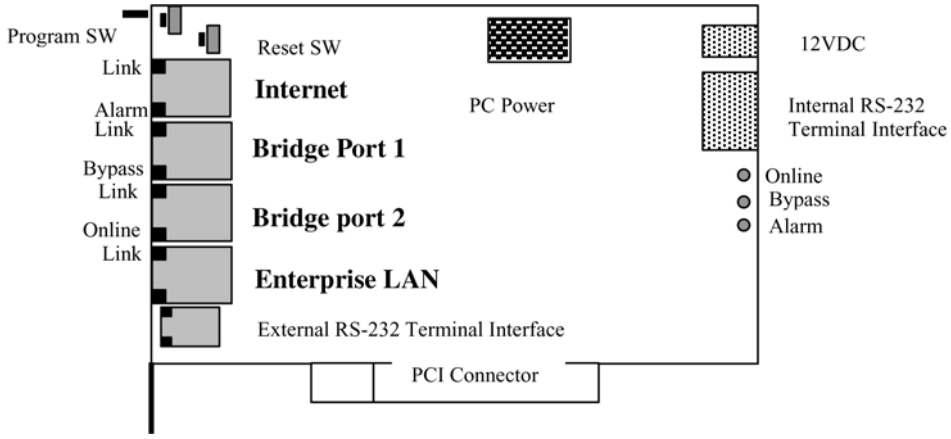
High Availability Module Setup

Overview

There are four steps involved in setting up the *H.A.M*. Each of these steps is outlined below:

1. Installing the *H.A.M*.
2. Identify the ports on the *H.A.M*.
3. Connect the *Internet* and *Enterprise LAN Ports*
4. Configure ContentKeeper to use the *H.A.M* via the *Web Interface*.

Note: If you are using an *SME Appliance* or an *LE Appliance* then the setup information for the *H.A.M* will appear in a table at the end of each section.



Installing the High Availability Module

There are three factors to consider when installing the *Internal H.A.M* PCI card. These are the location of the card within the appliance, how the card will receive power and how the appliance will interface with the card. Each of these issues is discussed below.

When installing an *External H.A.M*, the location and power supply factors are predetermined, so you only have to decide how the appliance will interface with the *External H.A.M*.

Location

The *Internal H.A.M* PCI card has been designed to be seated in a PCI slot within an appliance. Should there be an available PCI slot within the appliance, then it is recommended that the *H.A.M* be installed into this slot.

Although the *Internal H.A.M* is a PCI card, when installed into a PCI slot, it only uses the PCI bus to draw power. As the *H.A.M* has more than one power source, it is not strictly necessary to install it into a PCI slot.

However, some appliances are designed with more PCI card mounting points than actual PCI slots. If, for example, other devices take up all available PCI slots, the *H.A.M* may be installed into a blank mounting point (i.e. one that has no motherboard connector below it). In this configuration, plug a spare HDD power connector into the socket provided on the *H.A.M* to supply power to it.

Important: When installing the *H.A.M* into a blank mounting point, ensure that the PCI connector is completely insulated and no components or parts of the *H.A.M* PCI card are touching other components on the motherboard. Failure to do this may result in damage to the *H.A.M* or the appliance.

Appliance	Location
SME	If you are using a H.A.M with an *SME Appliance* then you will be using the external model, which will be located out side of the appliance. Note that you may wish to leave extra space above, below of behind the SME Appliance for the H.A.M when installing the SME Appliance in a rack.
LE	If you are using a H.A.M with an *LE Appliance* then you will be using the internal model, which will be located in the module upgrade port on the front panel.

Power

Power to the *H.A.M* may be supplied in one of three different ways, depending on where it is installed.

PCI Bus – If the *H.A.M* is installed into a motherboard PCI slot then it will draw power from the PCI bus. No PCI resources other than 5Volt power are utilised by the *H.A.M*.

PC Power – If the *H.A.M* is not installed into a blank PCI slot then it can receive power via a standard hard drive power connector.

External Power – If the *H.A.M* is not installed into a PCI slot then it can receive power via an external 12 Volt 300mA AC power supply (Centre positive, 2.1mm connector). The gigabit *H.A.M* requires the same power supply but rated at 500mA. If you are using an External H.A.M with your own manually built appliance, you must use the external power option.

Appliance	Power Supply
SME	If you are using a *H.A.M* with an *SME Appliance*, the power will be supplied via the serial interface cable connected to the serial connector on the rear panel.
LE	If you are using a *H.A.M* with an *LE Appliance*, the power will be supplied by the *LE Appliances* internal PCI bus.

Important: Do not supply the *H.A.M* with more than one source of power. Should there be a power failure, the *H.A.M* will automatically switch to *Bypass* mode.

Serial Interface

The *H.A.M* must be connected to the ContentKeeper server through one of its two available serial interface ports. Control of the *H.A.M* is accomplished via an RS-232 control interface. It should be noted that only one interface connection is required for proper operation. Available server resources and user preference will dictate the choice of interface connection. Refer to the following two sections as a guide when deciding which serial interface to use.

Appliance	Serial Interface
SME	If you are using a *H.A.M* with an *SME Appliance*, connect the *External H.A.M* DB9 serial interface to the serial connector on the rear panel.
LE	If you are using a *H.A.M* with an *LE Appliance*, then the *H.A.M* is connected to the *LE Appliance* via an internal serial interface.

External Interface

To establish a connection between the ContentKeeper appliance and the *External Interface*, a cable to connect the external RJ11 *Serial Interface Port* to one of the server's serial ports is required. The cable requires a specific wiring configuration.

Note: Refer to Appendix E in Chapter 6 for information on constructing such a cable.

Internal Interface

To establish a connection between the ContentKeeper server and the *Internal Interface*, a cable to connect the HAM internal Female DB9 *Serial Interface Port* to one of the server's serial ports is required. The cable requires a specific wiring configuration.

Note: Refer to Appendix E in Chapter 6 for information on constructing such a cable.

Identifying Ports on the H.A.M.

There are six ports on the *H.A.M*, an *Internet Port*, an *Enterprise LAN Port*, two *Bridge Ports* and external and internal *Serial Interface Ports*. The function of each port is described below.

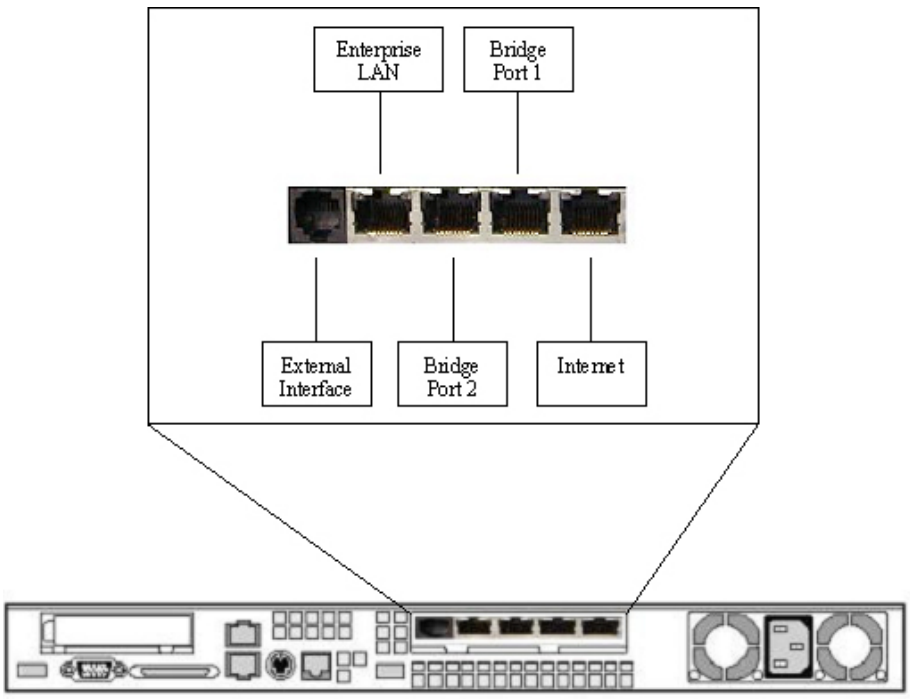
Internet Port – This port connects the *H.A.M* to the Internet via a network device such as a router. The port is of DCE type, and is labelled *Router* on the external model.

Enterprise LAN Port – This port connects the *H.A.M* to a network usually via a network device such as a HUB. This port is of DTE type, and is labelled *Switch* on the external model.

Bridge Ports – These ports connect the *H.A.M* to the ContentKeeper appliance. *Bridge Ports 1* and *2* on the *H.A.M* connect to *Bridge Ports 1* and *2* respectively, on the ContentKeeper server. These ports are of DCE type, and are labelled *Server 1* and *Server 2* respectively on the external model.

External Interface Port – This port is used for configuring the *H.A.M*, controlling link configuration and receiving status information. On the Internal and external models, the *External Interface Port* is an RJ11 socket and conforms to the RS-232 specification.

Internal Interface Port – This port serves the same function as the *External Interface Port*. The *Internal Interface Port* is a Female DB9 socket and conforms to the RS-232 specification. This port is also available externally on the external model of the *H.A.M*.



Connecting the Internet and Enterprise LAN ports

In order to provide an understanding of how and why specific cables must be used to connect the ports on the *H.A.M*, an explanation of each port type has been outlined below.

DCE – DCE is an acronym for Data Communications Equipment. The devices and connections of a communications network that connect the communication circuit between the data source and destination (the Data Terminal Equipment or DTE). A modem and a HUB are the most common kinds of DCE.

DCE and DTE are often connected by an RS-232 serial line. It is necessary to distinguish these two types of device because their connectors must be wired differently.

DTE – DTE is an acronym for Data Terminal Equipment. A device which acts as the source and/or destination of data and which controls the communication channel. DTE includes terminals, Ethernet cards and Routers.

Refer to the previous figure to identify each port on the *H.A.M*. The previous figure is a rear view of a server and represents a typical *Internal H.A.M* installation. The previous figure may also be used identifying ports on the *External H.A.M,* as it is very similar.

Note: The *External Interface Port* is smaller and inverted when compared to the Ethernet ports.

Identifying Cable Types

Important: The *Internet Port* and *Enterprise LAN Port* each require different types of cable when connecting to different network devices. Using the wrong cables will prevent the H.A.M. from passing Ethernet traffic.

Use UTP CAT5 or CAT6 cables (standard Ethernet cables) for connecting the *Internet Port* and *Enterprise LAN Port*.

Ethernet cables come in varying colours and lengths. The best way to differentiate between straight-thru and cross-over cables is to examine the wires in the plugs on each end of the cable. When doing this, make sure that both plugs are the same way up. Place the two cable ends side by side and examine the wires within:

Straight-Thru cables will have the wires in the same order in both ends.

Cross-Over cables will have the wires in a different order on either end.

Use the following table to determine the type of Ethernet cable to use with the *H.A.M*.

Internet Port Connected to:	Cable type:	Enterprise LAN Port Connected to:	Cable type:
Router	Straight-Thru	Router	Cross-Over
NIC	Straight-Thru	NIC	Cross-Over
Switch	Cross-Over	Switch	Straight-Thru
HUB	Cross-Over	HUB	Straight-Thru

Connecting the Bridge Ports

Always use Straight-Thru cables when connecting the *Bridge Ports* on the *H.A.M* to the *Bridge Ports* on the ContentKeeper appliance. Two straight-thru Ethernet cables are included with the *High Availability Module* kit.

Completing H.A.M Configuration

Upon installation, the *H.A.M* is in *Bypass* mode (its default state) and will remain so until all online conditions are met. The H.A.M. will automatically switch to *Online* mode when all online conditions are. This enables the administrator time to connect all cables and configure ContentKeeper before bringing it online.

Note: Refer to the Online Mode section in this chapter for a full description of all online conditions.

The final step in installing the *High Availability Module* is to configure ContentKeeper to use it. This operation is performed via the *ContentKeeper Web Interface* once ContentKeeper has been installed.

Note: For instructions on configuring the H.A.M, refer to the High Availability Module (H.A.M) section in Chapter 5.

Installing ContentKeeper

ContentKeeper may be installed with the *ContentKeeper Auto Installer*.

Important: Do not use the *ContentKeeper Auto Installer* on a ContentKeeper *SME Appliance* or an *LE Appliance* that has been supplied by ContentKeeper Technologies or a ContentKeeper channel partner.

Note: Refer to the Obtaining Evaluation Software section in the Introduction for more information on obtaining the *ContentKeeper Auto Installer*.

If you download the *ContentKeeper Auto Installer* ISO image, you will need to burn it to a blank CD in order to use it. Be sure to only use a permanent or CDROM marker when labelling CDs.

Using the ContentKeeper Auto Installer

1. Ensure that you have the necessary configuration information at hand and that there is a monitor and keyboard attached to the ContentKeeper appliance.

Note: Refer to the Obtaining Configuration Information section in this chapter for a list of the necessary configuration information.

2. Boot your ContentKeeper appliance with the *ContentKeeper Auto Installer*. Ensure that you understand the information presented on the welcome screen then type **`install`** and press **ENTER** to proceed.

Note: Refer to the Troubleshooting The Auto Installer section in Chapter 4 if you are having difficulty using a PS/2 keyboard with the *Auto Installer*.

3. Configure the time zone when prompted then click **next**.

   The *ContentKeeper Auto Installer* will proceed to install and configure Red Hat Linux.

4. Once the installation of Red Hat Linux has completed you will be prompted with the ContentKeeper *License Agreement*. Read and accept this agreement to enter the ContentKeeper *Setup Program*.

The ContentKeeper Setup Program

The ContentKeeper *Setup Program* may only be accessed from the Red Hat Linux command shell or during the execution of the *ContentKeeper Auto Installer*.

The purpose of the ContentKeeper *Setup Program* is to allow you to configure the IP address settings for the *Management Port* and the customer registration details.

The ContentKeeper *Setup Program* will start automatically during the execution of the *ContentKeeper Auto Installer,* once the license agreement has been read and accepted. The ContentKeeper *Setup Program* may also be run at any time to reconfigure the *Management Port* IP address settings.

Note: Refer to the Accessing the ContentKeeper Setup Program from the ContentKeeper Console Screen section and the Accessing the ContentKeeper Setup Program from the Remote Serial Console section in this chapter for more information on accessing the ContentKeeper *Setup Program*.

To use the ContentKeeper *Setup Program*, enter a valid value for each item. If the ContentKeeper *Setup Program* is being run from the *ContentKeeper Auto Installer* then a value must be entered for each item, otherwise you may press **ENTER** at any item to accept the current value.

You may press **H** followed by **ENTER** to view context sensitive help on any item in the *Parameter Configuration Settings* or the *Client Appliance Configuration Settings* sections.

You will be asked for the information on the following page when using the ContentKeeper *Setup Program*.

Parameter Configuration Settings
Device name for first bridging interface (H–Help) <eth0> :
Device name for management port (H–Help) <eth1> :
Device name for second bridging interface (H–Help) <eth2> :

Port Numbers for Filtering.
(Use '|' as separator), (H–Help) <80|8080|3128> :

Note: If you use a proxy server to access the Internet then you may need to enter the proxy server IP address and port number when prompted. Otherwise type “no” when prompted.

Client Appliance Configuration Settings
IP Address for management port (H–Help) <xxx.xxx.xxx.xxx> :
HostName (H–Help) <xxxxxxxxxxxx> :
Management port Netmask (H–Help) <xxx.xxx.xxx.xxx> :
Use Proxy (H–Help) <yes/no> :
Proxy IP Address (H–Help) <xxx.xxx.xxx.xxx> :
Proxy Port Number (H–Help) <xxxx> :
Gateway IP Address (H–Help) < xxx.xxx.xxx.xxx > :
DNS IP Address (H–Help) < xxx.xxx.xxx.xxx > :
Domain Name (H–Help) <null> :

Network Address : <xxx.xxx.xxx.xxx>
Broadcast Address : <xxx.xxx.xxx.xxx>

Do you want to use an SSL connection between the ContentKeeper Appliance and the ContentKeeper Web Interface ? (H–Help) <Yes> :

Note: In the section below you must enter a value for each question.

Customer Details
Your ContentKeeper Administrator's name <eg. Bill Smith> :
Your ContentKeeper Account's name <eg. Joe Bloggs> :
Your Company name <eg.Acme Company Inc.> :
Your Address 1 <eg. 21 Business Road> :
Your Address 2 <option> :
Your City <eg. Boston> :
Your State <eg M.A. > :
Your Zip Code <eg. 1234> :
Your Country <eg. USA> :
Your Telephone country code <eg. 1> :
Your Telephone area code <eg. 242 > :
Your Telephone number <eg. 62122424> :
Your Fax number <eg. 62579801> :
Your Email Address <eg. bill.smith@yourcompany.com> :
Reboot Machine to Start ContentKeeper
On next reboot execute ContentKeeper <yes> : **yes**
Reboot Machine <no> : **yes**

At the end of the ContentKeeper *Setup Program* you will be prompted to reboot ContentKeeper, unless you are running the ContentKeeper *Setup Program* from the *ContentKeeper Auto Installer* in which case you will be prompted to press any key to continue.

You should say yes to reboot ContentKeeper so that any new IP address settings may be applied, although when not running from the *ContentKeeper Auto Installer*, you may safely re-run the ContentKeeper *Setup Program* as many times as necessary.

Connecting the ContentKeeper Management Port

ContentKeeper will start when the appliance reboots and appear on the console screen as white text with a blue background. If you have not done so already, connect the *Management Port* to your network now. The following messages will appear at the bottom of the screen:

Waiting to register ContentKeeper!
Waiting on a response from DataCenter!
Failed contacting DataCenter! Trying every 5 minutes!

If the first two messages do not clear within 10 minutes or the last message does not clear within 15 minutes then this indicates that your network connectivity is incorrectly configured and ContentKeeper cannot connect to the Internet.

Note: Refer to Chapter 3 for more information on DataCenter Connectivity requirements and Management Port Location guidelines. If you are still unable to connect ContentKeeper to the *ContentKeeper DataCenter* then refer to the Troubleshooting section in chapter 4.

If ContentKeeper cannot connect to the Internet you may need to run the ContentKeeper *Setup Program* again and review your *Management Port* IP address settings.

Note: The Management Port IP address settings may also be viewed from the *Web Interface* in the *Appliance Configuration Settings* menu. Refer to Chapter 5 for more information on the Appliance Configuration Settings menu.

Note: The *Management Port* Proxy settings may also be viewed from the *Web Interface* in the *Management Port Proxy Settings* menu. Refer to Chapter 5 for more information on the Management Port Proxy Settings menu.

Accessing the ContentKeeper Setup Program from the ContentKeeper Console Screen

To access the ContentKeeper *Setup Program* from the *Console Screen*, first press **SHIFT-q** to exit from ContentKeeper then log on with a default username of **root** and a default password of **ck2001**. Next type **setup** and press **ENTER**.

Note: Refer to the Changing the Administration Passwords section in Chapter 4 for information on changing the default logon passwords.

Warning! Stopping ContentKeeper by pressing SHIFT-q will stop the ContentKeeper Bridge from passing traffic. If you are not using a H.A.M then this may lead to a network outage until ContentKeeper is restarted.

Accessing the ContentKeeper Setup Program from the Remote Serial Console

The process of accessing the ContentKeeper *Setup Program* from the *Remote Serial Console* is similar to the process of accessing it from the *Console Screen*.

Note: Refer to the Remote Serial Console section in this chapter for more information about using the *Remote Serial Console*.

To access the ContentKeeper *Setup Program* from the *Remote Serial Console*, first log on with a username of **root** and a password of **ck2001**. Next type **setup** and press **ENTER**.

Note: Refer to the Changing the Administration Passwords section in Chapter 4 for information on changing the default logon passwords.

Warning! Stopping ContentKeeper by pressing SHIFT-q will stop the ContentKeeper Bridge from passing traffic. If you are not using a H.A.M then this may lead to a network outage until ContentKeeper is restarted.

Remote Serial Console

The *Remote Serial Console* will only be enabled if there is a COM port available on the ContentKeeper appliance that does not have anything connected to it, such as the H.A.M.

Use the serial connector on the front of the *SME Appliance* and the *LE Appliance* for the *Remote Serial Console*.

Follow the procedure below to use the *Remote Serial Console*. The procedure details connecting a Microsoft Windows system to the *Remote Serial Console*, but the concepts and COM port settings may be applied to any system with terminal emulation software installed.

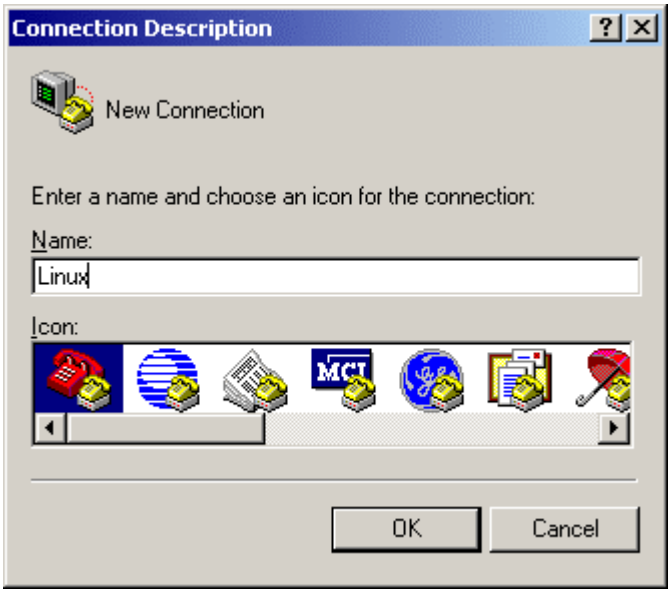
1. Plug a “serial cross-over cable” into your PC and also into the relevant COM port on the ContentKeeper appliance. This will be the front COM port on the *SME Appliance* and the *LE Appliance*.

Note: The ContentKeeper *SME Appliance* and the ContentKeeper *LE Appliance* come packaged with a black 2 M serial cross-over cable.

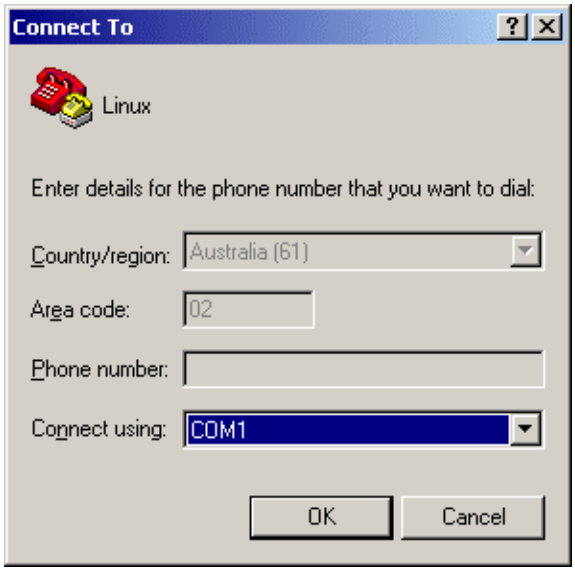
---

2. Open Hyper Terminal from **`Start > Programs > Accessories > Communications > Hyper Terminal`** or a similar menu.

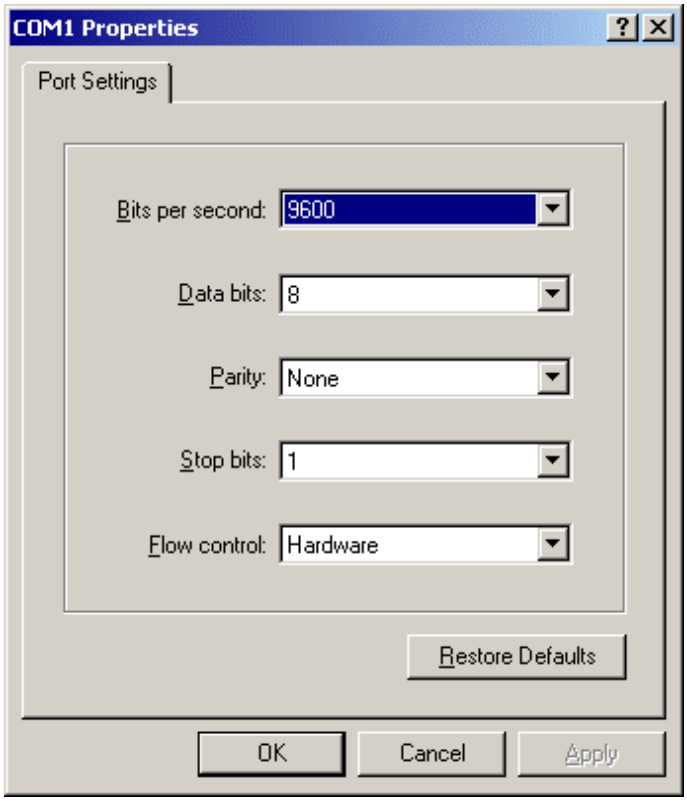
3. Give your new connection a name, E.g. **`Linux`**, and click “OK”.



4. Select the appropriate COM port and click “OK”.

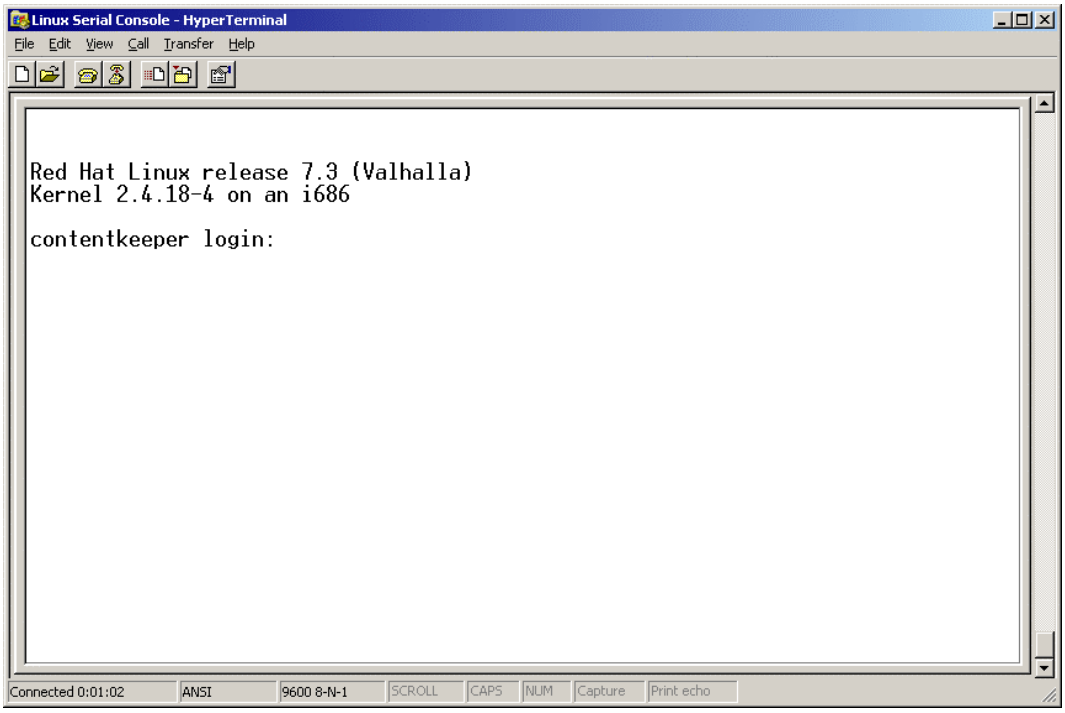


5. Configure the following settings, then click “OK”:
    - Bits per second: 9600
    - Data bits: 8
    - Parity: None
    - Stop Bits: 1
    - Flow control: Hardware



6. The session should connect when you click **OK** and Hyper Terminal should display **Connected** in the lower left corner. If not then from the **Call** menu, select **Call** to connect.

7. Press **ENTER** and Hyper Terminal should display the Red Hat Linux logon prompt.



Note: In the future you may have press **Enter** once connected to force a login prompt to be displayed. This is because when Linux boots it writes the login prompt to the COM port then when you plug your cable in and connect it is already waiting for a username. Pressing “Enter” just forces it to redisplay the login prompt.

Note: Refer to the ContentKeeper Default Logon Passwords section in Chapter 4 for more information on the default logon passwords.

Chapter 3

Deploying ContentKeeper

Chapter 3, *Deploying ContentKeeper*, is a detailed examination of the requirements for, and the procedures involved in deploying ContentKeeper into an organisation. It also contains guidelines and technical overviews of the deployment and integration of ContentKeeper into a network. This section will contain cross-referencing to other relevant sections within the Administration Guide.

Introduction

The contents of this chapter are targeted at the tasks most closely associated with deploying a ContentKeeper appliance into an organisation.

Note: Refer to Chapter 2 for information on obtaining or building a ContentKeeper appliance if you do not already have one.

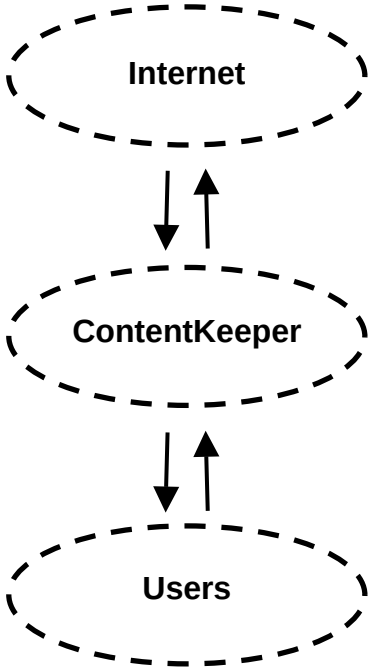
This chapter has been broken into two sections, *Planning to Deploy ContentKeeper*, and *Deploying ContentKeeper*. These two sections represent the two major phases of deploying ContentKeeper.

Before beginning to plan the deployment of ContentKeeper, it is essential that you understand the basic concept behind how ContentKeeper is able to perform filtering. It's pretty simple . . .

Conceptually, ContentKeeper is able to perform Internet filtering by sitting between users and their connection to the Internet so that all requests bound for the Internet must first pass through ContentKeeper. This way ContentKeeper is able to block any requests for inappropriate Internet content before they are serviced.

The physical reality of this concept is that ContentKeeper is a transparent adaptive Ethernet bridge able to pass any type of Ethernet traffic, and specifically designed to filter HTTP traffic, including proxy encapsulated and WCCP-GRE encapsulated traffic.

Use the following diagram to help you visualise and understand this concept.



Planning to Deploy ContentKeeper

This section examines the tasks involved in planning to deploy a ContentKeeper appliance. The primary focus when planning to deploy a ContentKeeper appliance is determining which networks ContentKeeper is going to filter and where, physically, the ContentKeeper appliance will be attached.

Note: Here is a good tip, use an accurate network diagram when planning to deploy ContentKeeper. Being able to visualise where the ContentKeeper appliance is to be physically deployed will be of great benefit.

Deployment Planning Guidelines

Use the following list as a guide when planning to deploy a ContentKeeper appliance. Each point in this list is discussed in more detail in the *Deployment Planning Overview* section below.

- Determine which network segments at your site are to be filtered.
- Determine whether there are any remote network segments to be filtered, such as VPNs or WAN links.
- Determine whether your site is using a proxy server, and whether users can bypass it.
- Determine the most appropriate location for the *ContentKeeper Bridge Ports*.
- Decide upon which subnet the *ContentKeeper Management Port* will be attached to.
- Determine the most appropriate method of *Username Resolution* for your site.

Deployment Planning Overview

This section examines in detail the tasks involved in planning to deploy a ContentKeeper appliance, and contains a discussion of each of the points presented in the *Deployment Planning Guidelines* section above. The sub-sections presented here directly correspond to items in the *Deployment Planning Guidelines* section, and appear in the same order as they are presented in the *Deployment Planning Guidelines* section.

Filtering of Local Network Segments

One of the first tasks in planning to deploy ContentKeeper is determining exactly which of your organisations network segments are to be filtered. For simplicities sake this task has been broken down into two separate tasks, *Filtering of Local Network Segments* (this section) and *Filtering of Remote Network Segments* (the next section).

The task of determining which of your organisations local network segments are to be filtered can usually be completed with a minimum of effort.

Pose yourself the question “How do the users in my organisation connect to the Internet?”. Answer this question and you will probably have completed the first task in planning to deploy ContentKeeper. Here are some points to consider along with the question:

- Do all of the departments within your organisation use the same Internet gateway?
- Does your organisation use a web caching proxy server?
- If your organisation uses a web caching proxy server, can it be bypassed?

Filtering of Remote Network Segments

As stated in the previous section, one of the first tasks in planning to deploy ContentKeeper is determining exactly which of your organisations network segments are to be filtered. This section looks at filtering of remote network segments.

If your organisation does not have any remote network segments then you can skip this section.

If your organisation does have remote network segments, such as VPNs, WAN links and remote dial-in users, then you will need to consider whether they also are to be filtered by ContentKeeper. Here are some additional points to consider:

- Do the users on your remote network segments use your local Internet gateway when connecting to the Internet?
- Do the users on your remote network segments use your local web caching proxy server when connecting to the Internet?
- If the users on your remote network segments use your local Internet gateway or proxy server when connecting to the Internet, do they also have alternative methods of connecting to the Internet that are local to them, such as those provided by a redundant Internet connection.

Filtering Proxy Server Traffic

Many organisations employ a web caching proxy server, commonly referred to as a proxy server. Because of this, the most common ContentKeeper deployment scenario, and the recommended deployment method, is where the ContentKeeper appliance is installed directly between the proxy server and the users.

As stated earlier in this chapter, ContentKeeper is a transparent adaptive Ethernet bridge able to pass any type of Ethernet traffic, and specifically designed to filter HTTP traffic, including proxy encapsulated and WCCP-GRE encapsulated traffic. Coupling this with the fact that ContentKeeper supports the Basic, NTLM and Digest proxy authentication schemes means that ContentKeeper may be deployed in almost any scenario involving proxy servers and transparent proxying.

Note: Refer to the CISCO WCCP-GRE Support section in this chapter for more information on deploying ContentKeeper in networks using WCCP-GRE for transparent proxying.

If your organisation uses a proxy server or multiple proxy servers, commonly known as a proxy server farm, then usually the most appropriate location for ContentKeeper is between the proxy server, or proxy server farm, and the users. However, if the users can access the Internet by bypassing the proxy server, then they will also be able to bypass filtering, i.e. ContentKeeper. If this is the case then you must consider alternatives, here are two suggestions:

- Force your users to access the Internet via your proxy server by configuring the Internet gateway, usually a firewall, to only accept Internet requests from your proxy server. This course of action will have the additional benefit of increasing your network security.
- Deploy ContentKeeper on your internal LAN, directly inside your Internet gateway (firewall). Taking this course of action may impact upon some of ContentKeepers features. This potential issue is examined below.

The advantage to deploying ContentKeeper between your proxy server and the users lies in ContentKeepers ability to directly filter the users URL requests, rather than filtering the proxy servers URL requests. When directly filtering user URL requests, ContentKeeper is able to see the source IP address of the request, and where proxy authentication is used, the username of the user who made the request. This impacts upon ContentKeepers ability to perform the following functions:

- Username Resolution
- URL request to policy matching (in terms of associating a policy with a user/IP address or group of users/IP addresses)
- Reporting (in terms of including usernames and IP addresses being included in reports)
- Excluded/Included IP addresses

If ContentKeeper cannot determine the source of URL requests, i.e. who made the URL request, then it is limited in how it may apply blocking rules (policies). Usually this results in one blocking rule being applied to the whole organisation.

Note: Refer to the ContentKeeper Management Port Location section in this chapter for more information on configuring the Management Port to use a proxy server.

Cisco WCCP-GRE Support

Web Cache Co-ordination Protocol (WCCP) facilitates the link between Cisco IOS-enabled routers and cache engines. Through WCCP, cache engines can be clustered to provide scalability and resiliency. The protocol allows one or more proxies to register with a single router to receive (WCCP-GRE encapsulated) redirected traffic. It also allows one of the proxies, the designated proxy, to dictate to the router how redirected traffic is distributed across the array.

Generic Router Encapsulation (GRE) is a tunnelling protocol developed by CISCO that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to CISCO routers.

WCCP and GRE are often used in conjunction with transparent HTTP proxy servers. It is important to note that standard GRE and WCCP-GRE have different protocol numbers. ContentKeeper natively supports automatic detection and filtering of WCCP-GRE encapsulated HTTP traffic. This feature requires no configuration or user intervention.

This enables ContentKeeper to effectively filter and block HTTP traffic when deployed on a network using WCCP-GRE.

Note: Refer to RFC 1701 and RFC 1702 for more GRE protocol specific details, as well as RFC 3040 for more WCCP protocol specific details.

ContentKeeper Bridge Port Location

Deciding upon the physical location of the *ContentKeeper Bridge Ports* is really what the *Planning to Deploy ContentKeeper* is all about. Once you have made this decision everything else (the method of *Username Resolution* that you use, your policy deployment strategy) will start to fall into place.

There is one golden rule that must be observed when deciding on where to attach you *ContentKeeper Bridge Ports* to your network. That rule, which is explained in the introduction to this chapter, is *“Web site requests must traverse the ContentKeeper Bridge in order for ContentKeeper to filter them”*.

There is another rule that must be observed when configuring ContentKeeper that is very similar to the first rule, *"ContentKeeper must be configured to monitor the TCP port on which Web site requests are being made".* If ContentKeeper is not configured to monitor HTTP traffic on the correct port this may reduce or completely prevent its ability to filter traffic.

Note: Refer to the General Parameters section in Chapter 5 for more information on configuring which TCP ports ContentKeeper is to monitor.

Once you have determined which network segments are to be filtered by ContentKeeper, and whether or not you are able to deploy ContentKeeper between your proxy server and the users, you will have a good indication of where you are going to attach the *ContentKeeper Bridge Ports* to your network.

Cabling the ContentKeeper Bridge Ports

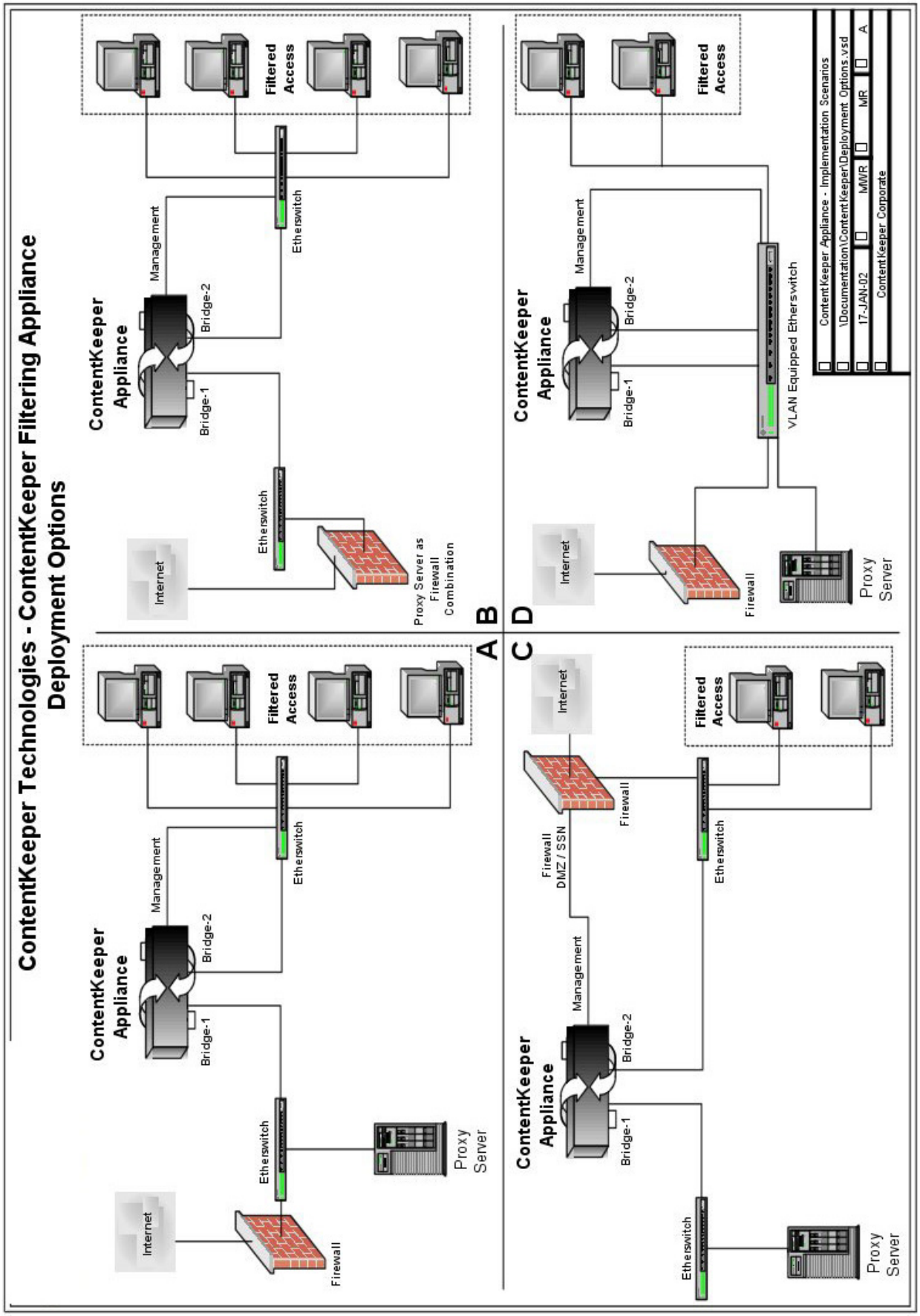
Use the following table as a guide when attaching the *ContentKeeper Bridge Ports* to your network.

Link Partner	Cable Type
Router	Cross-Over
NIC	Cross-Over
Switch	Straight-Thru
HUB	Straight-Thru
Auto polarity sensing Network Interface	Straight-Thru

Note: If you are using a H.A.M then refer to the Identifying Cable Types section in Chapter 2 for a guide to connecting the HAM ports to your network.

Example Deployment Scenarios

Refer to the network diagram on the following page for common examples of ContentKeeper deployment scenarios. While doing so, please note the use of a VLAN equipped ether-switch in example *Scenario D*.


ContentKeeper Technologies - ContentKeeper Filtering Appliance
Deployment Options
A
B
C
D
Filtered Access
ContentKeeper Appliance
Management
Bridge-2
Bridge-1
Etherswitch
Internet
Firewall
Proxy Server as Firewall Combination
Proxy Server
VLAN Equipped Etherswitch
Firewall DMZ / SSN
ContentKeeper Appliance - Implementation Scenarios
\Documentation\ContentKeeper\Deployment Options.vsd
17-JAN-02
MWR
MR
A
ContentKeeper Corporate

ContentKeeper Management Port Location

When configuring the *Management Port* and deciding upon the *Management Port* location, there are two important factors to consider. These are its ability to contact the *ContentKeeper DataCenter* and its ability to have network connectivity/visibility from the network clients (user workstations). These two factors are critical in ensuring the optimum performance of your ContentKeeper installation.

DataCenter Connectivity

Although the *ContentKeeper Adaptive Ethernet Bridge* will always pass Ethernet traffic, ContentKeeper must register with the *ContentKeeper DataCenter* before it will begin to filter. The simplest way to determine if ContentKeeper has registered with the *ContentKeeper DataCenter* is to examine the *Reg. ID* field on the console screen, or from the *Current Status* menu in the *ContentKeeper Web Interface*. If the value contained within the field is *New*, and/or is displayed in inverse video or bold red text then ContentKeeper has not registered with the DataCenter.

The *Management Port* must also be able to contact the *ContentKeeper DataCenter* on an hourly basis to retrieve *URL Database* updates. ContentKeeper does not usually include the URL database when installed. Downloading of the *URL Database* occurs over approximately six hours and is achieved via *Tricklefeed*™ process where the database is broken into small packages and downloaded by the ContentKeeper server. Using this process minimises the impact on available network bandwidth.

ContentKeeper will not perform any *Live Filtering* or *Control List Filtering* until the local *URL Database* has been completely downloaded. Examine the *DB-Status* field on the *ContentKeeper Console Screen*, or in the *Current Status* menu to determine how much of the *URL Database* has been downloaded.

If ContentKeeper is unable to contact the *ContentKeeper DataCenter* for thirty days, then it will deem the *URL Database* to be too far out of date and will stop filtering and blocking. The *ContentKeeper Adaptive Ethernet Bridge* will always continue to pass Ethernet traffic though.

Note: The *Management Port* may be configured to connect to the *ContentKeeper DataCenter* via a proxy server. Refer to the Management Port Proxy Settings section in Chapter 5 for instructions to configure the Management Port to use a proxy server.

Connectivity With Network Clients (User Workstations)

The *Management Port* performs several functions, two of which are IP based *Username Resolution* and receiving URL reclassification submissions from network clients. In order for the management port to perform these functions, it must have TCP/IP connectivity to the filtered network clients, specifically TCP and UDP port numbers 137,138,139 (for *Username Resolution*) and TCP port number 80 (For URL reclassification submissions and authenticated site / file type access (for the blue *Authenticate* screens)).

Username Resolution

ContentKeepers ability to perform *Username Resolution* is directly effected by the location of the *Management Port*. It is important that this consideration is taken into account when planning to deploy ContentKeeper.

Note: Refer to the Connectivity With Network Clients (User Workstations) section in this chapter for more information on how location of the *Management Port* affects ContentKeepers ability to perform *Username Resolution*.

Note: Refer to the Configuring Username Resolution section in Chapter 4 for information on the *Username Resolution* methods supported by ContentKeeper.

Deploying ContentKeeper

This section examines the tasks involved in deploying a ContentKeeper appliance. Included in this section are a set of guidelines and a procedure to follow when deploying a ContentKeeper appliance.

Deployment Guidelines

Use the following list as a guide when deploying a ContentKeeper appliance. Each point listed below is discussed in more detail in the *Deployment Overview* section below.

1. Ensure the ContentKeeper appliance has been sufficiently configured.
2. Prepare a location for the ContentKeeper appliance.
3. Deploy the ContentKeeper appliance.

Deployment Overview

This section examines in detail the tasks involved in deploying a ContentKeeper appliance, and contains a discussion of each of the points presented in the *Deployment Guidelines* section above. The sub-sections presented here directly correspond to items in the *Deployment Guidelines* section, and appear in the same order as they are presented in the *Deployment Guidelines* section.

Initial ContentKeeper Configuration

Before deploying ContentKeeper you should ensure that ContentKeeper is configured to suit your network environment. The following list indicates which features of ContentKeeper should be configured before it is deployed.

Note: Each item in the list is also discussed in the Initial Configuration section in Chapter 4.

- **Management Port** – The ContentKeeper *Management Port* IP address settings should be configured for the production network before ContentKeeper is deployed. It is often much more convenient to configure the *Management Port* in a test environment than after the ContentKeeper appliance has been installed into a rack and attached to a production network.

  Note: Refer to the ContentKeeper Management Port Location section in this chapter for a discussion of points to consider when connecting the ContentKeeper *Management Port*. Refer to The ContentKeeper Setup Program section in Chapter 2 for instructions to reconfigure the *Management Port* IP address settings.

- **DataCenter Connectivity** – ContentKeeper must be able to connect to the *ContentKeeper DataCenter* once it has been deployed. Pre-configure the *Management Port Proxy Settings* for your production network if they will be different to those used before ContentKeeper is deployed.

  Note: Refer to the DataCenter Connectivity section in this chapter for a discussion of why ContentKeeper must be able to connect to the *ContentKeeper DataCenter*. Refer to the Management Port Proxy Settings section in Chapter 5 for instructions on how to reconfigure the *Management Port Proxy Settings*.

- **High Availability Module** – If you are using a *H.A.M* with ContentKeeper, then ContentKeeper should be configured to use the *H.A.M* before it is deployed.

  Note: Refer to the High Availability Module (H.A.M.) section in Chapter 2 for more information on installing and connecting the H.A.M. Refer to the High Availability Module (H.A.M.) section in Chapter 5 for instructions on how to configure ContentKeeper to use the H.A.M.

- **Web Interface** – The default password for the *ContentKeeper Web Interface* should be changed before ContentKeeper is deployed to a production network. This is because the default password is published in this Administration Guide, on the Internet, and is easily obtainable by users.

  Note: Refer to the Change Administration Password section in Chapter 5 instructions on how to change the default *Web Interface* administration password.

- **Silent Mode** – If you have decided to use *Silent Mode*, then this should be enabled before ContentKeeper is deployed to a production network.

  Note: Refer to the Silent Mode section in Chapter 4 for a discussion of using ContentKeeper in *Silent Mode*. This section also contains links to instructions on how to configure *Global Silent Mode* and *Per-Policy Silent Mode*.

- **ContentKeeper Agent** – If the *ContentKeeper Agent* is being used, it should be deployed and configured before ContentKeeper is deployed to a production network.

  Note: Refer to the ContentKeeper Agent section in Chapter 5 for instructions on how to deploy and configure the ContentKeeper Agent.

- **Username Resolution** – *Username Resolution* should be configured before ContentKeeper is deployed to a production network.

  Note: Refer to the Configuring Username Resolution section in Chapter 4 for a discussion of ContentKeeper Username Resolution. Refer to the Username Resolution section in Chapter 5 for instructions on how to configure ContentKeeper *Username Resolution*.

- **Bridge Device Settings** – ContentKeeper *Bridge Device Settings* should be configured before ContentKeeper is deployed to a production network. This is especially true if the ContentKeeper appliance (or H.A.M) is to be attached to a network interface with fixed speed and duplex settings.

  Note: Refer to the Bridge Device Settings section in Chapter 5 for instructions on how to configure the ContentKeeper *Bridge Device Settings*.

Making Space for the ContentKeeper Appliance

Before you deploy ContentKeeper it is good practice to make space for the ContentKeeper appliance in your rack or machine room. It is also good practice to prepare any necessary network and power cables before deploying.

Being prepared will save you from running around trying to organise things at the last moment, which may well lead to an unsuccessful deployment.

Note: The *ContentKeeper SME Appliance* is a 1U (1 Rack Unit) appliance; the *ContentKeeper LE Appliance* is a 2U (2 Rack Unit) appliance, both come with a rack mounting kit. Refer to The ContentKeeper Appliance section in Chapter 2 for more information about the ContentKeeper SME Appliance.

Deploying the ContentKeeper Appliance

Use the following procedure as a guide when deploying ContentKeeper:

1. Ensure that you have read and understood this chapter.

2. Ensure that your ContentKeeper Appliance is sufficiently configured. Refer to the Initial ContentKeeper Configuration section in this chapter for more information.

3. Attach the *ContentKeeper Management Port* to the production network, and then boot the ContentKeeper appliance. Ensure that you can access the *ContentKeeper Web Interface*.

4. If you are using a *H.A.M* then proceed with *Step-a* below, otherwise proceed with *Step-b* below.

   a. Attach the *Internet Port* and the *Enterprise LAN* Port to the production network, and then attach the *H.A.M Bridge Ports* to the *ContentKeeper Bridge Ports*. DO NOT ATTACH THE *H.A.M* SERIAL CABLE (unless you are using in internal serial cable in

which case you must immediately browse to the *Web Interface* and force the *H.A.M* into *Bypass* mode).

b. Ensure that ContentKeeper is running, and then attach the *ContentKeeper Bridge Ports* to the production network.

5. Ensure that ContentKeeper has successfully connected to the *ContentKeeper DataCenter*. If you are using a *H.A.M* then connect the serial interface cable and force the HAM into *Online* mode.

6. Check the *RX Packets* and *RX Bytes* fields in the *Status Information* menu and ensure that there is traffic traversing the C*ontentKeeper Bridge*. You may have to refresh your browser a few times to confirm this.

7. Open a browser on a filtered network client (user workstation) and check that you have Internet access. Then browse to a URL that you know will be blocked and see if you get blocked by ContentKeeper. If you have deployed ContentKeeper in Silent Mode you will need to examine the *Current Blocking Activity* report to see if your request was blocked.

8. Return to the *ContentKeeper Web Interface* and examine the *Current Internet Activity* menu to confirm that URL requests from users are being logged, then browse to the *Current Blocking Activity* menu to confirm that your blocked request was logged. Also ensure that *Username Resolution* is working by checking for the presence of resolved usernames in both menus.

If you have reached this point and all of the steps in the above procedure have been successful, then congratulations, you have successfully deployed ContentKeeper. If you have not done so already, you should read Chapter 4 to familiarise yourself with general ContentKeeper administration and then complete the configuration of ContentKeeper.

If you have reached this point and not all of the steps in the above procedure have been successful, then you should refer to the Troubleshooting section in Chapter 4 to resolve any issues before repeating the procedure.

Chapter 4

Administering ContentKeeper

The purpose of Chapter 4, *Administering ContentKeeper*, is to describe ContentKeeper management practices and troubleshooting procedures. The contents are largely conceptual or procedural with a heavy emphasis on referring to other sections of the Administration Guide for detailed information. There will be very comprehensive cross-referencing to other relevant sections within the Administration Guide

ContentKeeper Administration Overview

This chapter aims to familiarise the reader with the concepts and procedures associated with administering ContentKeeper.

The chapter starts out with an introduction to administering ContentKeeper then looks at how *ContentKeeper Blocking* works, and the remainder of the chapter is taken up with overviews and common procedures of configuration, general management, reporting and troubleshooting.

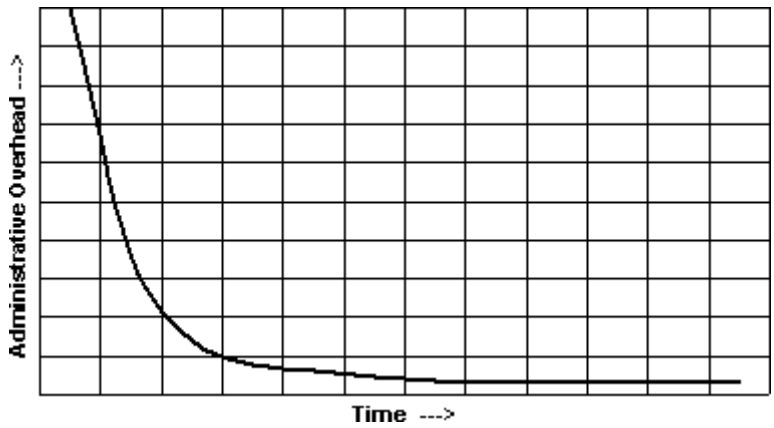
As mentioned in the synopsis, the contents of this chapter are largely conceptual or procedural with a heavy emphasis on referring to other sections of the Administration Guide for detailed information. All of the references in this chapter and throughout the Administration Guide are hyperlinks to the specified section. An index is also provided for easy reference.

What's involved in administering ContentKeeper?

ContentKeeper usually requires very little administration. The initial deployment and configuration account for most of the administrative overhead associated with ContentKeeper. Once ContentKeeper has been deployed and configured the associated administrative overhead decreases rapidly.

The reason for this is that the biggest jobs associated with ContentKeeper are (1) deciding on where to attach ContentKeeper to your network, (2) configuring *Policies* and (3) configuring *Username Resolution*, and all of these tasks are performed during the initial deployment.

After ContentKeeper is up and running with *Policies* configured, the maintenance and administration of ContentKeeper is minimal. This graph demonstrates how the administrative overhead associated with ContentKeeper rapidly decreases after the initial deployment.



The few tasks that remain once ContentKeeper has been deployed are mostly tasks that have already been performed during the initial deployment and configuration, such as modifying policies. This contributes to the simplicity of administrating ContentKeeper.

The sort of tasks that you can expect to perform once ContentKeeper has been deployed fall into one of the following three categories:

- Managing Policies
- Managing Authentication
- Managing URL Reclassification
- Monitoring Activity Reports

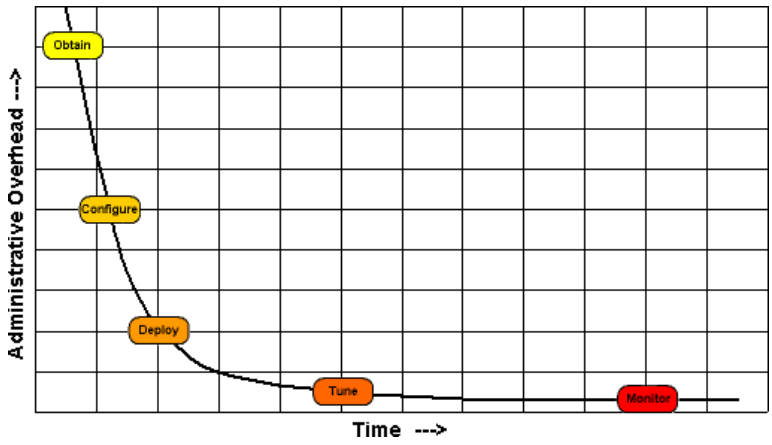
The next section will examine these tasks more closely, along with the ContentKeeper administration life cycle.

The ContentKeeper Administration Life Cycle

ContentKeeper has a well-defined administration life cycle, which can be broken into five phases as depicted in the following diagram.

The first three phases of the administration life cycle can be said to occur during the initial deployment of ContentKeeper, the fourth phase occurs directly after the initial deployment of ContentKeeper and the fifth and final phase is an ongoing phase that begins after the fourth.

If we superimpose the *Administrative Overhead graph* with the *ContentKeeper Administration Life Cycle diagram* we can begin to see why the administrative overhead associated with ContentKeeper rapidly reduces over time.



Note: Chapter 3 contains a procedural overview of the first three phases of the *ContentKeeper Administration Life Cycle*, where each of the phases is described in detail. Refer to Chapter 3 for more information.

Let us examine in some detail each of the phases of the *ContentKeeper Administration Life Cycle*.

Phase 1

The first phase of the *ContentKeeper Administration Life Cycle* involves obtaining a ContentKeeper appliance, which may be achieved by purchasing an *SME* or *LE* appliance with *ContentKeeper Technologies* or one of its channel partners.

Note: Refer to The ContentKeeper Appliance section in Chapter 2 for more information on the *ContentKeeper SME* and *ContentKeeper LE* appliances.

Alternatively you may build your own ContentKeeper appliance on any Intel architecture with the *ContentKeeper Auto Installer*.

Note: Refer to Chapter 2 for instructions on how to build your own ContentKeeper appliance.

Phase 2

The second phase of the *ContentKeeper Administration Life Cycle* involves performing the initial configuration of the ContentKeeper appliance.

Note: Refer to the Configuring ContentKeeper section in this chapter for a discussion on configuring ContentKeeper including some procedures.

The purpose of the configuration performed during this phase is to allow ContentKeeper to be connected to your network for the purpose of registration, as well as to allow monitoring of users current browsing habits to assist in the design of *Custom Policies*. This configuration will be tuned and completed during phase four.

Note: Refer to the Initial ContentKeeper Configuration section in Chapter 3 for a detailed list of features to configure as part of the initial configuration.

Phase 3

The third phase of the *ContentKeeper Administration Life Cycle* involves deploying the ContentKeeper appliance. This includes installing the ContentKeeper appliance into a rack or computer room, attaching the *Bridge Ports* and reconfiguring *Management Port* connectivity.

Note: Refer to Chapter 3 for more information on deploying ContentKeeper.

Phase 4

The fourth phase of the *ContentKeeper Administration Life Cycle* involves tuning your ContentKeeper configuration. This may include such activities as:

- Creating *Custom Policies*
- Configuring the *Log Offloader*
- Configuring *Blockpage Customisation*
- Creating *Departmental Reports Accounts*

Generally by this phase, with the exception of creating *Custom Policies*, all of the large configuration tasks have been completed.

Note: Refer to Configuring ContentKeeper section in this chapter for more information about configuring ContentKeeper.

Phase 5

The final phase of the *ContentKeeper Administration Life Cycle* begins once ContentKeeper has been completely configured and involves the ongoing monitoring of Internet usage for Internet access management purposes.

This phase may also include some tuning of policies as organisational requirements change, but will mostly involve reporting and URL reclassification.

Note: Refer to ContentKeeper Reporting section in this chapter for more information about ContentKeeper reports.

ContentKeeper Filtering Explained

In this section we will examine *ContentKeeper Filtering* in detail. A ContentKeeper appliance is a transparent adaptive Ethernet bridge able to pass any type of Ethernet traffic (routable or non-routable), and specifically designed to filter HTTP traffic, including proxy encapsulated and WCCP-GRE encapsulated traffic. ContentKeeper must be deployed on a network between the users and their Internet gateway in order to properly filter Internet content.

Note: A web caching proxy server is a valid user Internet gateway.

ContentKeeper filtering works by ContentKeeper intercepting each URL request and filtering it based upon a set of rules, known as a policy. ContentKeeper may be configured with many sets of rules, up to one hundred in fact. When ContentKeeper intercepts a URL request it must decide upon which set of rules to apply to the request, this process is known as *Policy Matching*.

To perform *Policy Matching*, ContentKeeper must first be able to uniquely identify each URL request; it does this by associating each request with its source, which may be an *IP Address* or a *Username*. Once ContentKeeper has uniquely identified the URL request it matches it to the policy that is targeted at the requests source.

ContentKeeper *Policies* consist of *Policy Components*; these include a *Directory Service*, *Directory Objects*, *Categories*, *File-Types* and *Custom URLs*. ContentKeeper uses *Directory Objects* to match URL requests. A *Directory Object* may be an IP address or range of addresses, a username or a group of usernames.

Once ContentKeeper has matched a URL request to a policy it then applies the access rules within that policy to the request to determine how the request is to be filtered.

ContentKeeper has two special policies, the *Default Policy* and the *Global Policy*. The *Default Policy* is always enabled and has no *Directory Service* or *Directory Objects* associated with it. Any URL request is automatically matched to the *Default Policy*, unless it is matched to a *Custom Policy* as determined by *ContentKeeper Policy Logic*.

Note: Refer to The Default Policy and The Global Policy sections in this chapter for more information about how the *Default Policy* and the *Global Policy*.

ContentKeeper Policy Logic and *Policy Implementation Requirements* are explained in the following section.

Policy Logic And Implementation Requirements

Policies rely on ContentKeeper's ability to accurately determine user and computer identities. ContentKeeper does this through *Username Resolution*.

Network users may be identified in two ways, user credentials (which include a user name and a group name) and computer credentials (IP addresses and DNS names).

User credentials may be ascertained in the following ways:

- Extracted from the header of a http-get request [sent to a proxy server that requires authentication]
- Retrieved via an IDENT lookup request
- Retrieved via an eDirectory lookup request
- Retrieved via a NetBIOS lookup request

Computer credentials may be ascertained in the following ways:

- Retrieved via a NetBIOS lookup request
- Retrieved via a DNS lookup request

NT4/W2K Domain membership may be ascertained in the following ways:

- Extracted from the header of a http-get request

Once credentials have been ascertained, they must be matched to a policy, specifically a *Directory Object* within a policy. This may be achieved in varying ways, depending on how *ContentKeeper Username Resolution ContentKeeper Policies* and are configured.

ContentKeeper may attempt to match credentials against the following types of *Directory Object* within a policy:

- IP address and subnet mask.
- Username and/or group from the local database.
- Username and/or group from a Windows NT/2000 security group.
- Username and/or group from a Novell eDirectory security group.
- Username and/or group from an LDAP compliant directory service.

Both the IP address / subnet mask and local database data sets are stored locally on the ContentKeeper appliance. The *ContentKeeper Agent* supplies ContentKeeper with Windows NT/2000 security group data from a Windows NT/2000 domain controller. eDirectory and LDAP data is enumerated from a specified server by ContentKeeper at start-up and stored locally on the ContentKeeper appliance.

Refer to the Configuring Username Resolution section in this chapter for more information on the available Username Resolution methods and how to choose the most appropriate method for your organisation.

Once ContentKeeper has confirmed and matched the user or computer credentials it will apply the appropriate policy.

When implementing *ContentKeeper Policies*, the following requirements and rules must be observed:

1. Each unique username may exist in only one policy when entered into the *username* field.

2. Each unique username may exist in multiple policies when entered via the *group* field.

3. Each IP address and 32-bit subnet mask combination may exist in only one policy. An example of an IP address and 32-bit subnet mask combination is *203.5.115.24 / 255.255.255.255*.

4. When a policy is created, all upper case letters will be converted to lower case in the name, description and object fields.

A URL request may qualify for filtering if either it's source IP address or the embedded user name match one of those in a policy. All other requests will be filtered through the *Default Policy*, with the exception of those whose source IP addresses are specifically set to exclude in the *Excluded/Included IP Addresses* menu.

Refer to the Excluded/Included IP Addresses section in Chapter 5 for more information about configuring *Excluded/Included IP Addresses*.

If a URL request qualifies for filtering through at least one policy other than the default, then none of the default policy settings are applied when filtering takes place.

A URL request may qualify for filtering through multiple policies when either its source IP address or the embedded user name exists in more than one policy. When a URL request qualifies for filtering through multiple policies, generally the least restrictive policy settings apply with the exception of *Category Settings* versus *File-Type Settings* in which case the most restrictive settings apply.

The tables on the following page outline ContentKeepers *Policy Logic*.

ContentKeeper decides how to filter a URL request based on the following priorities (in the order that they are presented here):

(1)Global Priorities	
Priority Order	**Directive**
1	Requests from excluded IP addresses are not filtered.
2	If the default only check box is enabled then only the default policy is applied.

(2)Policy Choice Priorities	
Priority Order	**Directive**
1	Any policy containing an IP address and 32-bit subnet mask that match the IP address of the request is applied exclusively.
2	Any policy containing a username that matches the username embedded in the request is applied exclusively.
3	Any policies with groups that contain a username that matches the username embedded in the request are applied collectively.

(3)Policy Component Priorities	
Priority Order	**Directive**
1	Custom and Trusted URLs
2	Category States
3	Custom File Types

(4)Category Priorities	
Priority Order	**Directive**
1	Block
2	Authenticate
3	Coach
4	Allow

Closed Loop Collaborative Filtering

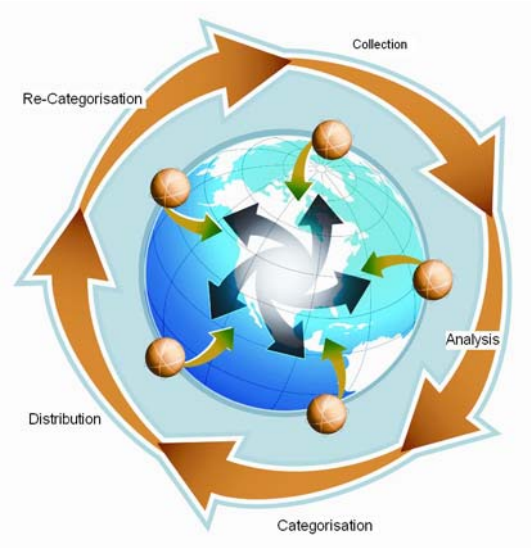
ContentKeeper uses *Closed Loop Collaborative Filtering*™ technology which insures that ContentKeeper is superior in it's ability to manage and control Internet access. *Closed Loop Collaborative Filtering*™ is ContentKeepers closed circuit system designed to collect, analyse, categorise, edit and distribute URLs worldwide.

ContentKeeper units in the field are designed to poll the *ContentKeeper DataCenter* hourly to receive *Control List* updates of newly discovered and processed URLs. During this process, any new suspect URLs discovered locally are encoded, encrypted, compressed and sent back to the *ContentKeeper DataCenter* for anonymous submission to our AI (Artificial Intelligence) analysis and categorisation engines. Sites that are then confirmed to fall into one of the control categories are added to the *Control List* updates then collected automatically by every ContentKeeper unit in the field.

This means (for example) that when a ContentKeeper user in New York browses to a new URL that contains pornography, ContentKeeper users worldwide will have the benefit of that update usually within 2 hours of the discovery being made.

Closed Loop Collaborative Filtering™ also allows ContentKeeper administrators to help maintain and edit the existing *Control List*. ContentKeeper administrators worldwide have the ability to instantly block, unblock and re-classify any site from their local ContentKeeper appliance. Reclassified URLs are sent back to the *ContentKeeper DataCenter* for manual review and *Control List* correction (if necessary).

The following diagram illustrates the concept behind the *Closed Loop Collaborative Filtering*™ process.



Collection → Analysis → Categorisation → Distribution → Re-Categorisation

Live Filtering

ContentKeeper employs real-time analysis and categorisation engines that automatically categorise any URL filtered by ContentKeeper that is not currently in the *URL Database*. This process is referred to as *Live Filtering*.

Any previously undiscovered URL that is *Live Filtered* will be categorised and entered into the *URL Database* within sixty seconds. Any further requests made to that URL, including those made by the original requester, will be filtered according to the settings being applied to the category under which the URL has been entered.

During this process, any new suspect URLs discovered locally are encoded, encrypted, compressed and sent back to the *ContentKeeper DataCenter* for anonymous submission to the AI (Artificial Intelligence) analysis and categorisation engines. This forms part of the *Closed Loop Collaborative Filtering*™ process.

Blocking Fundamentals

In this section we will examine ContentKeeper *Blocking Types* and *Blocking States* in detail. ContentKeeper provides three primary *Blocking Types* and four primary *Blocking States*. *Blocking Types* define how ContentKeeper targets Internet content (URLs), while *Blocking States* define how ContentKeeper processes Internet content (URLs). All of the *Blocking States* may be applied to each of the different *Blocking Types*. There are also some variations of the primary *Blocking States*.

All *Blocking Types* and *Blocking States* are individually detailed in the following sections. Variations of the primary *Blocking States* will be indicated where appropriate.

Blocking Types

ContentKeeper supports three primary *Blocking Types*. These are *Control List* based, *File-Type* based and *Custom URL* based. Each *Blocking Type* defines a unique method that ContentKeeper may use to target Internet Content (URLs).

The three primary blocking types defined below are:

- Control List
- File-Types
- Custom URLs

Control List

Through the use of the *Control List* blocking type ContentKeeper is able to target URLs by content type. This is possible because of *Categories* in the *Control List* (*ContentKeeper URL Database*).

The *ContentKeeper URL Database* contains millions of URLs grouped by type into thirty-two separate *Categories*.

Note: Refer to the Closed Loop Collaborative Filtering section in this chapter for more information about how the *ContentKeeper URL Database* is kept up to date. Refer to Appendix B in Chapter 6 for a definition of each of the Categories in the *ContentKeeper URL Database*.

An administrator is able to configure ContentKeeper to target a specific content type through the use of the *Categories* facility in the *Create & Edit Policies* menu.

Note: Refer to the Configuring Categories section under the Create & Edit Policies section in Chapter 5 for more information about configuring *Categories* for ContentKeeper.

Unique Categories

ContentKeeper processes the *Educational*, *News*, *Search Sites*, *Government Blocking List* and *Business Oriented* categories differently to its other categories. The blocking rules associated with each of these categories are outlined below.

Government Blocking List, Education, News & Search Sites – If a URL exists in any of these categories, it will be filtered according to the settings of that category, regardless of whether it is also categorized under another category.

Business Oriented – This category has been added to help ensure that business sites are correctly classified. URLs in this category are subject to two default rules:

1. URLs in this category are excluded from the real-time analysis engine.

2. If a URL exists in any **one** of the *Educational*, *News*, *Search Sites*, *Government Blocking List* and *Business Oriented* categories, it will be filtered according to the settings of that category, regardless of whether it is also categorized under another category.

When a URL belongs to more than one of the categories mentioned above then the order of priority of those categories is (1) *Government Blocking List*, (2) *News*, (3) *Search Sites*, (4) *Business Oriented* and (5) *Educational*.

For Example: If a URL is categorised under the *Government Blocking List* category as well as the *Entertainment* category and the *Government Blocking List* category is set to *Block* then the URL will be blocked regardless of what state the *Entertainment* category is set to.

File-Types

Through the use of the *File-Types* blocking type ContentKeeper is able to target URLs by file type. This is achieved via categorisation, or typing, of files by their extension, e.g. .exe, .bat, etc.

Important: *File-Type* filtering only applies to files being downloaded via the HTTP protocol (i.e. via an Internet browser), and not other protocols such as FTP.

An administrator is able to configure ContentKeeper to target a specific file type through the use of the *File-Types* facility in the *Create & Edit Policies* menu. The main use of this facility is filtering of file downloads.

Note: Refer to the Configuring File-Types section under the Create & Edit Policies section in Chapter 5 for more information about configuring *File-Types* for ContentKeeper.

Custom URLs

Through the use of the *Custom URLs* blocking type ContentKeeper is able to target a specific URL or group of URLs. This is achieved via the application of URL patterns and wildcards.

An administrator is able to configure ContentKeeper to target a specific URL or group of URLs through the use of the *Custom URLs* facility in the *Create & Edit Policies* menu.

Note: Refer to the Configuring Custom URLs section under the Create & Edit Policies section in Chapter 5 for more information about configuring *Custom URLs* for ContentKeeper.

Use the *Custom URLs* facility to define a list of individual URLs and associated *Blocking States*. *Custom URL Settings* will override *Category Settings* for the specified URLs. E.g. suppose that the *Sports* category is set to *Block* and the URL *www.sport.com* is in the *Custom URLs* list and set to Allow. If someone were to attempt to browse to *www.sport.com,* they would be allowed access, whereas all other sports sites would be blocked.

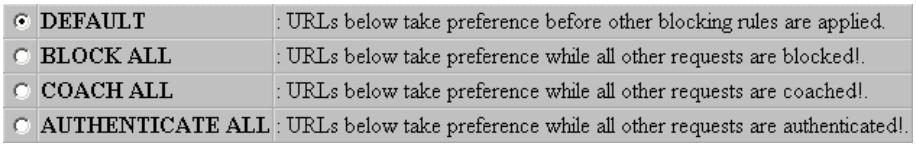
Entries in the *Custom URLs* menu will also override entries in the *File-Types* menu. E.g. suppose that *exe* extensions are set to *Block* in *File Types* and the

file *update.exe* is set to allow in Custom URLs. If someone were to attempt to download *update.exe*, they would be allowed access to the file.

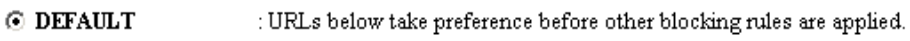
Important: In the *Custom URLs* menu, ContentKeeper treats .com as a URL component, not a file extension.

Mode of Operation

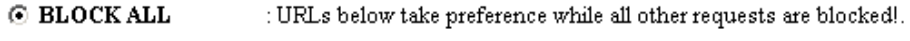
At the top of the *Custom URLs* screen there are four options. These options govern how ContentKeeper processes URLs for the current policy. Any URL specified under this feature will be processed accordingly and not processed as part of the normal categories. An explanation of each option follows.


DEFAULT : URLs below take preference before other blocking rules are applied.
BLOCK ALL : URLs below take preference while all other requests are blocked!.
COACH ALL : URLs below take preference while all other requests are coached!.
AUTHENTICATE ALL : URLs below take preference while all other requests are authenticated!.

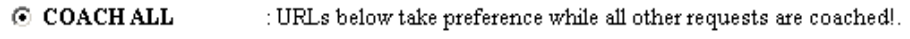
Important: The Option specified here will effect how ContentKeeper processes all URLs for the current policy.



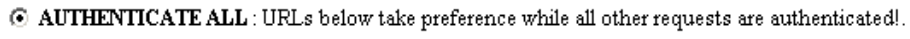
Selecting this option will cause ContentKeeper to process the URLs listed below in the specified manner (i.e. Allow, Block, Coach or Authenticate). ContentKeeper will process any URLs that do not match the Custom and Trusted URL list according to the Category States list.



Selecting this option will cause ContentKeeper to process the URLs listed below in the specified manner (i.e. Allow, Block, Coach or Authenticate). ContentKeeper will block any URLs that do not match the Custom and Trusted URL list.



Selecting this option will cause ContentKeeper to process the URLs listed below in the specified manner (i.e. Allow, Block, Coach or Authenticate). ContentKeeper will coach any URLs that do not match the Custom and Trusted URL list.



Selecting this option will cause ContentKeeper to process the URLs listed below in the specified manner (i.e. Allow, Block, Coach or Authenticate).

ContentKeeper will authenticate any URLs that do not match the Custom and Trusted URL list.

Custom IP Address and URL Entry Rules

IP address and URL entries in the *Custom URLs* facility are governed by certain rules. Refer to the Configuring Custom URLs section under the Create & Edit Policies section in Chapter 5 for more information about custom IP address and custom URL entry rules.

Blocking States

ContentKeeper supports four primary *Blocking States*. These are *Allow*, *Coach*, *Authenticate* and *Block*. Each *Blocking State* defines a unique method that ContentKeeper may use to process Internet content (URLs).

All of the *Blocking States* may be applied to each of the different *Blocking Types*. There are also some variations of the primary *Blocking States*, which are *Block Discard*, *Time of Day* and *Personal Surfing Units*. These variations allow the primary *Blocking States* to be applied in a flexible manner.

The *Blocking States* defined below are:

- Allow
- Coach
- Authenticate
- Block
- Block Discard
- Time of Day
- Personal Surfing Units

Allow

When a *Blocking Type* is processed with the *Allow Blocking State*, access to that *Blocking Type* will be granted.

For example, when a *Category* is set to the *Allow Blocking State*, any requests to URLs classified under the *Category* will be allowed by ContentKeeper and users will be able to access them.

Any Internet content that matches a *Category*, *File-Type* or *Custom URL* that is set to *Allow* will not be blocked, and will therefore be displayed on the computer that requested it.

Coach

When a *Blocking Type* is processed with the *Coach Blocking State*, access to that *Blocking Type* will be coached by ContentKeeper and the requesting users will be presented with a green *Coaching blockpage*. On the *Coaching blockpage* users will be asked to refer to their organisations acceptable Internet use policy and provided with a hyperlink to the requested URL.

Clicking on the provided hyperlink will redirect the users browser to the requested URL; however, once the users browser has been redirected a sixty-second time will be started within ContentKeeper. The user must navigate within the target URL before the sixty seconds elapses to avoid being presented with another *Coaching blockpage*.

In other words, if a user does not click anything on the target web page within the sixty seconds, the next time that they do click something, they will be presented with another *Coaching blockpage*.

Any Internet content that matches a *Category*, *File-Type* or *Custom URL* that is set to *Coach* will be blocked and a *Coaching blockpage* will be displayed on the computer that requested it.

Authenticate

When a *Blocking Type* is processed with the *Authenticate Blocking State*, access to that *Blocking Type* will be authenticated by ContentKeeper and users will be presented with a blue *Authentication blockpage*.

Users must enter a valid username and password in order to access the requested URL. If a user successfully authenticates, their browser will be redirected to the requested URL and they will not be required to authenticate again for the duration of the browser session (for that URL).

Any Internet content that matches a *Category*, *File-Type* or *Custom URL* that is set to *Authenticate* will be blocked and an *Authentication blockpage* will be displayed on the computer that requested it.

Block

When a *Blocking Type* is processed with the *Block Blocking State*, access to that *Blocking Type* will be denied and users will be presented with a red *blockpage*.

Any Internet content that matches a *Category*, *File-Type* or *Custom URL* that is set to *Block* will be blocked and a red *blockpage* will be displayed on the computer that requested it.

Block Discard

When a *Blocking Type* is processed with the *Block-Discard Blocking State*, access to that *Blocking Type* will be denied and users will be presented with a red *blockpage*.

The *Block-Discard Blocking State* is the same as the *Block Blocking State* with the exception that the block event is reported to the *Discarded Blocking Activity Report Log*, instead of the *Current Blocking Activity Report Log* where all other blocking events are reported.

Note: To view the *Discarded Blocking Activity Log*, select *View/Download Report Logs* from the *Current Status* menu in the *Web Interface*, and then click on the hyperlink for the *Discarded Blocking Activity Log*

Any Internet content that matches a *Category*, *File-Type* or *Custom URL* that is set to *Block-Discard* will be blocked and a red *blockpage* will be displayed on the computer that requested it.

Time Of Day

When a *Blocking Type* is processed with the *Time of Day (T.O.D) Blocking State*, access to that *Blocking Type* will be allowed or denied depending on the *Time of Day Settings*.

The *T.O.D Blocking State* allows an administrator to specify, via the *Time of Day Settings*, during which hours of the day a particular *Blocking Type* will be processed by a particular *Blocking State.*

Any Internet content that matches a *Category*, *File-Type* or *Custom URL* that is set to *T.O.D* may be processed with the *Allow*, *Coach*, *Authenticate*, *Block* or *Block-Discard Blocking States*.

Personal Surfing Units

When a *Blocking Type* is processed with the *Personal Surfing Units (P.S.U) Blocking State*, access to that *Blocking Type* will be allowed or denied depending on the *Personal Surfing Unit Settings*.

Personal Surfing Units allow an administrator to control access to Internet content types based on time usage. In more practical terms, this means that ContentKeeper can be configured to allow an individual or group access to a specified content type or types for a nominated period of browsing activity.

Any Internet content that matches a *Category* that is set to *P.S.U* may be processed with the *Block, Allow*, *Coach* or *Authenticate Blocking States*.

Configuring ContentKeeper

This section contains conceptual and procedural information about configuring ContentKeeper. The tasks discussed in the following sections include determining where to start configuration, performing the initial configuration and tuning your configuration. All of these tasks are then discussed in further detail in their own sections.

Note: Refer to Chapter 5 for more specific information on configuring each of ContentKeeper's features.

Where to Start

The purpose of this section is to assist you in determining how you should go begin the process of configuring and deploying ContentKeeper, whether you have just started reading the ContentKeeper Enterprise Administration Guide and do not yet have a ContentKeeper appliance, or if you have already deployed a ContentKeeper appliance on your network and want to know what to do next.

Use the following table to determine where you are in the ContentKeeper Administration Life Cycle and what actions you should take next.

Current Stage	Action
You are new to ContentKeeper.	Read the Introduction at the start of the ContentKeeper Enterprise Administration Guide.
You have seen an overview of ContentKeeper and want to learn more about how it works.	Read the ContentKeeper Administration Overview section followed by the ContentKeeper Filtering Explained section in Chapter 4.
You have just obtained a ContentKeeper appliance.	Read the Quickstart Guide in Chapter 1.
You have connected to the *Web Interface* and are ready to learn about deploying ContentKeeper.	Read the Planning to Deploy ContentKeeper section in Chapter 3.
You are ready to perform the initial configuration and deploy your ContentKeeper appliance.	Read the Deploying ContentKeeper section in Chapter 3.
You have deployed your ContentKeeper appliance and are ready to tune the configuration.	Read the Configuring Username Resolution section followed by the Configuring Policies section in Chapter 4.
Your ContentKeeper appliance is fully operational and filtering your organisation. Now you would like to learn more about monitoring Internet usage with ContentKeeper.	Read the Managing ContentKeeper section followed by the ContentKeeper Reporting section in Chapter 4.

Configuration Overview

This section, including the *Initial Configuration* and *Tuning Configuration* sections, forms an overview of the process of configuring ContentKeeper.

It is desirable to separate the process of configuring ContentKeeper into two phases, (1) *Initial Configuration* and (2) *Tuning Configuration*. The purpose of performing configuration in this way is twofold.

Firstly, by separating the task into two phases, which do not have to be performed together, it makes the task more manageable. Secondly, it allows ContentKeeper to be deployed in such a way that you are able to observe real-world Internet access data from your organisation, and you are able to see the effects of configuring different *Username Resolution* methods as well as the effects of configuring various *Policy Components*.

Deploying ContentKeeper in *Silent Mode* enhances this twofold purpose by allowing you to make configuration changes without affecting Internet access for your organisation or users.

Note: Refer to the Silent Mode section in this chapter for more information on deploying ContentKeeper in *Silent Mode*.

Initial Configuration

The initial configuration should be performed before ContentKeeper has been deployed, i.e. before the *Bridge Ports* have been connected to your production network.

The purpose of the initial configuration is to prepare ContentKeeper for deployment on your production network. The tasks involved in performing the initial configuration are outlined below, and each is discussed in more detail later in this chapter.

- Configure the *Management Port*.
- Access the *Web Interface*.
- Configure *Management Port Proxy Settings* and the time and date on the ContentKeeper appliance, and then establish connectivity with the *ContentKeeper DataCenter*.
- Configure the *High Availability Module* (optional).
- Connect to the *Web Interface* and change the default password.
- Enable *Silent Mode*.
- Configure *Excluded/Included IP Addresses*
- Configure the *Bridge Device Settings*.
- Configure *General Parameters*.

Tuning Configuration

Tuning of the ContentKeeper appliance configuration should be performed after ContentKeeper has been deployed. The tasks involved in tuning the configuration are outlined below, and each is discussed in more detail later in this chapter.

- Configure Logging.
- Configure *Username Resolution*.
- Configuring Custom Policies.
- Configuring *URL Reclassification Settings*.
- Configuring *Live Filtering Settings*.

Configuration Tasks

In this section each of the configuration tasks listed in the *Initial Configuration* and *Tuning Configuration* sections above are discussed in detail.

Configuring the Management Port

Proper configuration of the *ContentKeeper Management Port* is critical in ensuring the optimum performance of your ContentKeeper installation.

The *Management Port* may be configured or reconfigured with *the ContentKeeper Setup Program*.

Note: Refer to The ContentKeeper Setup Program section in Chapter 2 for more information about using the *ContentKeeper Setup Program* to configure the *Management Port* IP address settings.

There are a number of important factors to consider when deciding upon which network segment to attach the *Management Port* to.

Note: Refer to the ContentKeeper Management Port Location section in Chapter 3 for a discussion of points to consider when connecting the ContentKeeper *Management Port*.

There are other factors relating to the *Management Port* to consider when deploying ContentKeeper, and as such certain steps should be included in the initial configuration.

Note: Refer to the Initial ContentKeeper Configuration section in Chapter 3 for more information about configuring the *Management Port* when deploying ContentKeeper.

The ContentKeeper Web Interface

The *ContentKeeper Web Interface* is the main configuration interface for ContentKeeper. The *Web Interface* can be accessed from a workstation with an Internet browser, by browsing to ContentKeeper via its *Management Port* IP address or host name.

Note: You must be using DNS locally on your network with the hostname of the ContentKeeper appliance entered into the DNS server in order to be able to browse to ContentKeeper via its *Management Port* host name.

Accessing the Web Interface

The *Web Interface* may be accessed from any Internet browser via standard HTTP or via 128bit SSL encrypted HTTPS. You may configure ContentKeeper to use either HTTP or HTTPS with the *ContentKeeper Setup Program*.

Note: Refer to The ContentKeeper Setup Program section in Chapter 2 for more information about using the *ContentKeeper Setup Program*.

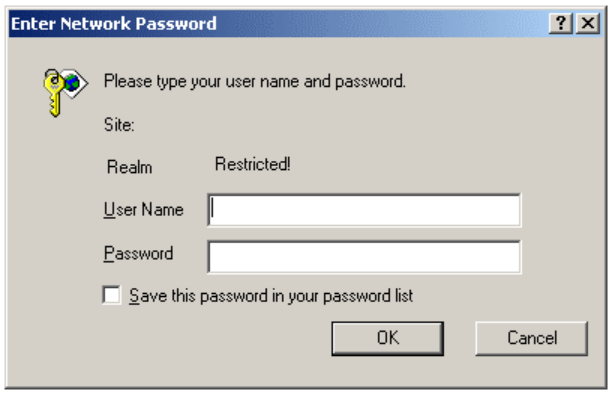
If you have configured ContentKeeper to use SSL encryption for the Web Interface, you will be presented with a *Security Alert* upon browsing to the *Web Interface*. The *Security Alert* notifies you of the impending secure connection and asks if you wish to proceed with the connection using the certificate presented by ContentKeeper. Click the *Yes* button to proceed, or click the *View Certificate* button to view ContentKeeper's security certificate.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

Note: If you have not configured ContentKeeper to use SSL encryption for the *Web Interface*, you will not be presented with a *Security Alert* upon browsing to the Web Interface.

Whether or not you are using SSL encryption, when you browse to ContentKeeper you will be presented with a logon window, enter a *Username* and *Password* then click *Ok* to access the *Web Interface*.

Note: Refer to the ContentKeeper Default Logon Password section in this chapter for a complete list of default logon usernames and passwords.



Logging Out Of The Web Interface

Click on the *Logout* hyperlink at the top and bottom of the *Web Interface* to securely log out of the *ContentKeeper Web Interface*. This will log out of the current *Web Interface* session and force any further access attempts to require re-authentication.

ContentKeeper Default Logon Accounts

By default there are three ContentKeeper logon accounts. Each account has its own password that is separate and independent of the other accounts and their passwords. Each account also has its own username that is separate and independent of the other accounts.

Important: All usernames and passwords are case sensitive.

When a ContentKeeper appliance is built and shipped by ContentKeeper Technologies or a channel partner, the usernames and passwords are preset, as outlined in the table on the following page.

ContentKeeper Default Logon Accounts		
ContentKeeper Web Interface	Username	admin
	Password	ck2001
ContentKeeper Console Screen	Username	root
	Password	ck2001
Remote Serial Console	Username	root
	Password	ck2001
Remote Access	Username	ckadmin
	Password	ck2001

Alternatively, when a ContentKeeper appliance is build by an end user, that person has the opportunity to specify the password for the console screen and remote access logons.

Note: Refer to Chapter 2 for more information about building a ContentKeeper appliance.

Changing the Administration Passwords

The *Web Interface* logon password may be changed in the *Change Administration Password* menu in the *Web Interface*.

Note: Refer to the Change Administration Password section in chapter 5 for instructions on how to change the *Web Interface* logon password.

The console screen and remote access passwords may be changed by logging on to the console with a username of root then entering the following command (replace the *username* with the appropriate value i.e. *root* or *ckadmin* and do not enter the brackets <>):

`passwd <username i.e. root or ckadmin>`

Enter and confirm the new password when prompted.

Browser Refresh Settings

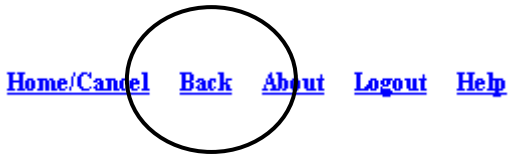
To ensure that the information being displayed is current, any browser from which you configure ContentKeeper should be set to check for newer versions of a page every visit. Refer to your browser's online documentation for help with configuring this feature.

Menu Navigation

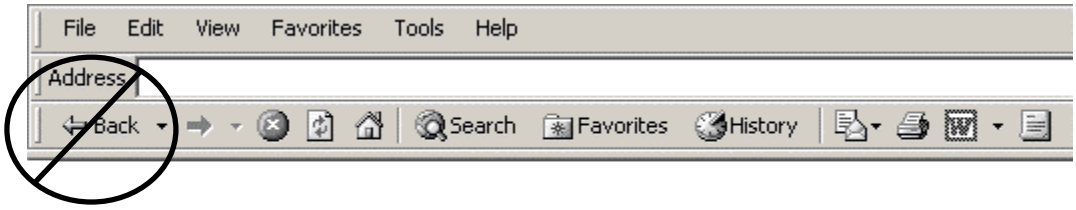
When navigating the menus of the *ContentKeeper Web Interface*, always use the ContentKeeper *Back* button as opposed to the browsers back button, because Internet browsers will cache the web pages that they display. In most cases, irrespective of refresh settings, when the browsers back button is clicked the last web page that was browsed to is displayed from the local cache. This will usually cause the browser to display information that is no longer current.

However, clicking the ContentKeeper *Back* button will force the browser to request a new page from the ContentKeeper server rather than displaying a locally cached page.

Use the ContentKeeper *Back* button



Not the browser *Back* button



Connecting ContentKeeper to the DataCenter

ContentKeeper must be able to connect to the *ContentKeeper DataCenter* in order to function properly. Although the *ContentKeeper Bridge* will always pass network traffic, it will not filter URL requests until ContentKeeper has registered with the *ContentKeeper DataCenter* and completely downloaded the *URL Database*.

Note: Refer to the DataCenter Connectivity Status section in Chapter 3 for more information about why ContentKeeper must be able to connect to the *DataCenter*.

The final step of installing ContentKeeper when building a ContentKeeper appliance, and one of the first steps to be performed when configuring a newly acquired appliance is allowing ContentKeeper to connect to the *ContentKeeper DataCenter* and register.

Note: Refer to the Connecting the Management Port section under The ContentKeeper Setup Program section in Chapter 2 for more information about registering ContentKeeper with the *ContentKeeper DataCenter*.

The current *DataCenter Connectivity Status* may be viewed from the *Status Information* menu in the Web Interface and from the Console Screen.

Note: Refer to the DataCenter Connectivity Status section under the Status Information section in Chapter 5 for more information about viewing the current *DataCenter Connectivity Status*.

The ContentKeeper *Management Port* may be configured to connect to the *DataCenter* through a proxy server.

Note: Refer to the Management Port Proxy Settings section in Chapter 5 for more information about configuring the ContentKeeper *Management Port* to connect to the *DataCenter* through a proxy server.

If your organisation employs an authenticating proxy server that does not support basic authentication, it may be necessary to bypass authentication for the ContentKeeper *Management Port*, or you may have to configure your network gateway to allow outbound HTTP connections from the ContentKeeper *Management Port*.

Note: If the ContentKeeper *Management Port* has been configured to connect to the *DataCenter* through a proxy server, but is unable to do so, it will attempt to connect directly through its network gateway.

ContentKeeper also requires connectivity to the *DataCenter* to retrieve hourly *URL Database* updates and submit URL reclassification requests.

Note: Refer to the URL Reclassification Settings section in Chapter 5 for more information about configuring how ContentKeeper will submit URL reclassification requests.

The Administration Guide includes troubleshooting procedures to assist you in diagnosing and resolving *DataCenter* connectivity issues.

Note: Refer to the Troubleshooting DataCenter Connectivity section in this chapter for more information.

Configuring the HAM

The ContentKeeper *High Availability Module (H.A.M)* is an optional extra available in internal and external models for both Fast Ethernet (10/100 Mbps) and Gigabit UTP (1000 Mbps) networks.

Note: Refer to the Obtaining Evaluation Software section in the Introduction for more information about obtaining a *High Availability Module*.

The *H.A.M* is designed to prevent ContentKeeper from becoming a single point of failure in a network by monitoring the ContentKeeper appliance and electrically bypassing the appliance if it fails.

The *H.A.M* is easily integrated with both pre-built and manually built ContentKeeper appliances.

Note: Refer to the High Availability Module (H.A.M) section in Chapter 2 for more information about installing and connecting the *High Availability Module*.

ContentKeeper must be manually configured to use the *H.A.M* through the *High Availability Module (H.A.M)* menu in the *ContentKeeper Web Interface*.

Note: Refer to the High Availability Module (H.A.M) section in Chapter 5 for more information configuring ContentKeeper to use the *High Availability Module*.

The Administration Guide includes troubleshooting procedures to assist you in diagnosing and resolving *H.A.M* issues.

Note: Refer to the Troubleshooting the H.A.M section in this chapter for more information.

Enabling Silent Mode

Note: Refer to the Silent Mode section in this chapter for more information about configuring and enabling *Silent Mode*.

Excluded/Included IP Addresses

The ContentKeeper *Excluded/Included IP Addresses* facility allows you to explicitly include or exclude from filtering, IP addresses, IP address ranges and even entire networks.

Note: Refer to the Excluded/Included IP Addresses section in Chapter 5 for instructions on how to configuring the ContentKeeper *Excluded/Included IP Addresses* facility.

IP addresses of workstations, servers and other network devices that you do not wish to be filtered should be entered into the *Excluded/Included IP Addresses* table and set to exclude before ContentKeeper is deployed. Some examples of network devices that you may not wish to be filtered are anti-virus servers, domain controllers and proxy servers.

Important! When ContentKeeper is deployed between a proxy server and the rest of the network, the proxy server IP address should be excluded from filtering. This prevents ContentKeeper from filtering URL requests made by

the proxy server, as ContentKeeper is designed to block inappropriate requests on their way to the proxy server from the users.

Note: Refer to the Deployment Scenario One section under *Step Four* of the *Quickstart Guide* in Chapter 1 for a more detailed description of this scenario including a network diagram.

Configuring Bridge Device Settings

Correct configuration of the *ContentKeeper Bridge Ports* is essential to the proper functioning of ContentKeeper. The *ContentKeeper Bridge Ports* must both be connected to network devices at the same speed and duplex whether they are directly connected, or connected via the *H.A.M*.

Failing to correctly configure the *ContentKeeper Bridge Ports* may cause ContentKeeper to contribute to reduced network throughput or completely prevent ContentKeeper from bridging network traffic altogether.

The current state of the *Bridge Ports* may be viewed from the *Status Information* menu in the *Web Interface*.

Note: Refer to the Bridge Port Status section under the Status Information section in Chapter 5 for more information about viewing the *Bridge Port Status*.

Use the following table as a guide when connecting the *ContentKeeper Bridge Ports*. The information in the following table is of a general nature and may not apply to your network devices. Refer to the manufacturer documentation for information specific to your network devices.

Device	Supported Speed	Supported Duplex
HUB	10/100 Mbps	Half
Switch	10/100 Mbps	Half, Full
NIC (Router/Firewall/Server)	10/100 Mbps	Half, Full
Note: This information does not apply to Gigabit capable devices.		

Important! It is not uncommon for network devices to have the speed and duplex of their network interfaces forced to a particular setting. If ContentKeeper is connected to such a device, then both of the *Bridge Ports* as well as the other device to which the *Bridge Ports* are connected must also be forced to the same speed and duplex settings.

Note: Refer to the Bridge Device Settings section in Chapter 5 for instructions on how to configure the *Bridge Port* speed and duplex.

When ContentKeeper is installed on an appliance that contains supported NICs, extra options become available in the *Bridge Device Settings* menu that allow you to manually configure the speed and duplex of the *ContentKeeper Bridge Ports*.

Note: Refer to the Supported Network Interface Cards section in Chapter 2 for a list of the NICs that are currently supported by ContentKeeper.

General Parameters

The ContentKeeper *General Parameters* menu allows you to specify on which TCP ports ContentKeeper will filter traffic. Correct configuration of the *General Parameters* menu is essential to the proper functioning of ContentKeeper.

When performing the initial configuration or planning to deploy ContentKeeper, determine on which TCP ports URL requests can be made, and then configure the *General Parameters* menu with those ports.

Note: Refer to the General Parameters section in Chapter 5 for instructions on how to configure the *General Parameters* menu.

If your organisation uses a proxy server then ContentKeeper will most likely be deployed between the proxy server and the network clients. In this scenario ContentKeeper may only need to be configured with the port number on which the proxy server is listening. Most proxy servers listen on ports 80, 8080 or 3128.

Important! When configuring ContentKeeper for use with a proxy server it is important to determine whether your network clients can bypass the proxy server when accessing the Internet. If this is the case then you must either prevent the network clients from bypassing the proxy server or deploy ContentKeeper to a point in the network where it will be able to filter requests that come directly from the network clients and requests that come via the proxy server.

If your organisation does not uses a proxy server then ContentKeeper will most likely be deployed between your Internet gateway and the network clients. In this scenario ContentKeeper may only need to be configured with the standard HTTP port number of 80.

Note: Be sure to remove any unnecessary port numbers from the *General Parameters* menu.

Configuring Logging

ContentKeeper log files can grow at a fast rate, particularly when ContentKeeper is deployed in large organisations. Ensure that ContentKeeper logging is configured correctly for your site by regularly reviewing the information presented in the *Report Log Settings* tables and adjusting the *Log File Age* setting when appropriate.

Note: Refer to the View/Download Report Logs section in Chapter 5 for instructions on how to view the *Report Log Settings* tables and configure the *Log File Age*.

ContentKeeper appliances usually have limited storage space, anywhere from forty to one hundred and sixty gigabytes. It is not uncommon for large sites to generate a larger volume of log files than there is storage space to hold them. ContentKeeper includes a *Log Offloader* to allow log files to be stored remotely to ContentKeeper. This can also be useful for log file archiving purposes.

Note: Refer to the Log Offloader section in Chapter 5 for instructions on how to configure the ContentKeeper *Log Offloader*.

Configuring Username Resolution

ContentKeeper relies on *Username Resolution* for reporting and policy matching purposes. Failing to correctly configure *Username Resolution* may mean that only IP addresses appear in reports and can be used for policy matching.

Note: Refer to the Username Resolution section in Chapter 5 for a complete list and explanation of each of ContentKeeper's *Username Resolution* methods.

Important! Some *Username Resolution* methods, such as NetBIOS and DNS, rely on configuration of operating systems or network services external to ContentKeeper and do not always result in 100% accurate *Username Resolution*.

Always test perform tests when selecting a *Username Resolution* method. Each of ContentKeeper's *IP Address* mode *Username Resolution* methods comes with it's own testing facility, while testing of *Proxy Header* mode *Username Resolution* may only be performed in a live scenario.

Configuring Policies

ContentKeeper allows you to create and manage filtering policies.

Filtering policies allow an administrator to have a high degree of control over how ContentKeeper filtering is applied to network users.

By using policies an administrator may tailor different filtering rules to meet the needs of different individuals and groups within an organisation. Policies may be assigned to individual users or groups of users, individual IP addresses or whole networks.

ContentKeeper *Policies* may also be used in conjunction with ContentKeepers *Included/Excluded IP Addresses* facility. This provides a powerful and effective method of filtering TCP/IP traffic from multiple networks or network segments.

These features allow ContentKeeper to effectively perform filtering across multiple organisations, and make it a powerful tool for large enterprises, ISPs and ASPs alike.

Note: Refer to the Included/Excluded IP Addresses section in Chapter 5 for more information on using the *Included/Excluded IP Addresses* facility.

There may be up to one hundred policies defined within ContentKeeper.

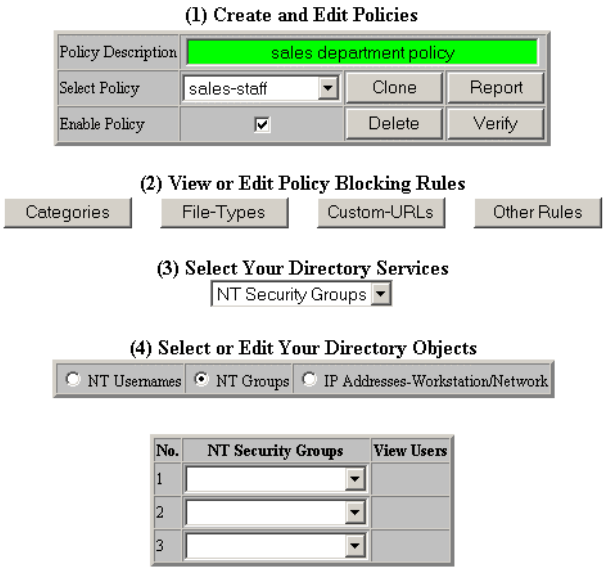
An Overview of ContentKeeper Policies

When ContentKeeper is first installed the only policy defined is the *Default Policy*. All traffic passing through ContentKeeper is filtered through this policy.

Note: Select *Create & Edit Policies* from the *Blocking/Reporting* menu in the *Web Interface* to configure policies.

Policies consist of the following components:

- Policy Name
- Policy Description
- Category states
- Custom file types
- Custom and trusted URLs
- Blocking rules
- Directory service objects



Each policy will have it's own settings for the different components.

Creating Custom Policies

The first step in configuring policies is to determine whether the default policy is sufficient or whether your organisation will require multiple policies.

When this box is **checked** ☑ only the **default** policy can be customized.
In this case the **default** policy is automatically applied to all requests.

To create multiple custom policies, the default only check box must be cleared.

When this box is **unchecked** ☐ you can clone (create), delete and customize multiple policies.
To create a new policy click on the "Clone" button (Maximum 100 Policies).

The process of creating custom policies can be broken into six steps, four of which can be seen in the *Create & Edit Policies* menu. The *Create & Edit Policies* menu has been designed to simplify this process by presenting each step in sequential order. These steps will now be described.

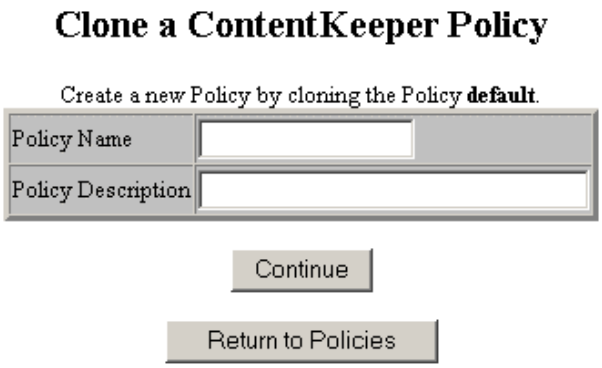
1. Create and Edit Policies (Clone an existing policy)
2. View or Edit Policy Blocking Rules
3. Select Your Directory Services
4. Select or Edit Your Directory Objects
5. Verify / Test the New Policy
6. Enable the Policy

Each of the above steps is expanded upon below. The number of each step below denotes relevance to a step above.

Note: The *Default Policy* and the *Global Policy* behave differently from *Custom Policies*. Refer to The Default Policy section and The Global Policy section in this chapter for more information.

1. Create and Edit Policies (Clone an existing policy)

Multiple policies are created by cloning an existing policy and then modifying the details of the new policy.



Note: Policy names may only contain the following characters:

- The numbers 0 to 9
- Upper and lower case letters A to Z and a to z
- The underscore character _
- The hyphen character –

Policy names may **not** contain spaces.

Once a new policy has been created, a directory service must be chosen. When configured, this will associate the policy with one or more users. Choosing a directory service will be discussed in the section "*3. Select Your Directory Service*" below.

Note: Refer to the Policy Cloning – Creating Custom Policies section in Chapter 5 for instructions on how to use the *Create & Edit Policies* menu to clone policies.

2. View Or Edit Policy Blocking Rules

Each policy component may be reconfigured at any time.

Categories

There are thirty-two *ContentKeeper Categories* which each represent a different type of Internet content. Use *ContentKeeper Categories* to configure which types of Internet content ContentKeeper will allow and which types it will block.

Note: Refer to the Configuring Categories section in Chapter 5 for instructions on how to configure *ContentKeeper Categories*. Refer to the Blocking Types section under the ContentKeeper Filtering Explained section in this chapter for a definition of *ContentKeeper Categories*.

Certain categories have unique rules applied to them. It is important to understand these rules and how they effect ContentKeeper filtering.

Note: Refer to the Unique Categories section in this chapter for an explanation of unique categories within ContentKeeper.

File-Types

Use *ContentKeeper File-Types* to configure filtering of file downloads via HTTP, i.e. files downloaded via an Internet browser.

Note: Refer to the Configuring File-Types section in Chapter 5 for instructions on how to configure *ContentKeeper File-Types*. Refer to the Blocking Types section under the ContentKeeper Filtering Explained section in this chapter for a definition of *ContentKeeper File-Types*.

Custom URLs

Use *ContentKeeper Custom URLs* to define a list of individual URLs and associated *Blocking States*. *ContentKeeper Custom URLs* combine the concepts of a *White List* and a *Black List* into one feature by allowing you to specifically allow or block each URL entry.

Note: Refer to the Configuring Custom URLs section in Chapter 5 for instructions on how to configure *ContentKeeper Custom URLs*. Refer to the Blocking Types section under the ContentKeeper Filtering Explained section in this chapter for a definition of *ContentKeeper Custom URLs*.

Other Rules

Use the settings in the *Other Rules* menu to enable or disable blocking and reporting for the current policy.

Click the *Save and Redisplay* button after making changes to apply the new configuration to ContentKeeper.

ContentKeeper Rules for Policy : default
Policy Rules
Report Blocked URLs in Blocking Activity Report
Yes
Generate a Blocking Page if URL Blocked
Yes
Remember to click on Save and Redisplay after making changes.
Save and Redisplay
Return to Policies
Note: When Generate Blocking Page is set to No
ContentKeeper will not block a given URL under this Policy.
Set this option to No to operate in slient mode while developing Policies.

Note: Refer to the Configuring Other Rules section in Chapter 5 for instructions on how to configure *Other Rules* for policies.

3. Select Your Directory Services

A directory service is a database of usernames, passwords and other information (objects) commonly used to authenticate users on a local area network (e.g. Microsoft NT Security Groups & Active Directory, LDAP, Novell NDS, RADIUS etc)

Currently ContentKeeper supports Windows NT/2000 security groups, Novell eDirectory (NDS), LDAP compatible directory services and its own local directory service.

There are currently four options available when choosing a directory service. Choose one appropriate to the network to which the policy will be applied.

Local Database – This option tells ContentKeeper to use information about users and groups that is stored in a database on the ContentKeeper server. User and group information must be entered manually. User information is entered via the Directory Objects table in the *Create & Edit Policies* menu, while group information is entered via the *Local Groups* menu.

Note: Refer to the LOCAL Groups section in Chapter 5 for instructions on how to configure *Local Groups* for use with policies.

NT Security Groups – This option tells ContentKeeper to use information about users and groups from a Windows domain, which has been supplied to it by the *ContentKeeper Agent*.

Note: Refer to the ContentKeeper Agent section in Chapter 5 for instructions on how to install and configure the *ContentKeeper Agent* for use with policies.

LDAP – This option tells ContentKeeper to use information about users and groups from an LDAP compatible directory service. This may be any LDAP compatible directory service, including those running in Microsoft, Novell and Unix environments. ContentKeeper only supports basic authentication when binding to an LDAP compatible directory tree.

Note: Refer to the LDAP/eDirectory Groups section in Chapter 5 for instructions on how to configure LDAP connectivity for use with policies.

eDirectory (NDS) – This option tells ContentKeeper to use information about users and groups from a Novell eDirectory. ContentKeeper only supports basic authentication when binding to a Novell eDirectory.

Note: Refer to the LDAP/eDirectory Groups section in Chapter 5 for instructions on how to configure Novell eDirectory connectivity for use with policies.

Once a directory service has been chosen, click the *Save and Redisplay* button at the bottom of the menu to send the new configuration to ContentKeeper, and continue configuring the policy.

4. Select Or Edit Your Directory Objects

Directory Services contain *Directory Objects*. *Directory Objects* are items such as usernames, passwords, IP addresses, groups and networks. *Directory Object* configuration instructions for each available *Directory Service* are outlined below.

Configuring Local Database Directory Objects

The *Local Database Directory Service* contains three types of *Directory Object*: usernames, local groups and IP addresses. A policy may contain one or more of each type of object.

Usernames - To modify the list of username objects associated with a policy, select the *Usernames* radio button to display the *Usernames* input field then type or cut and paste a maximum of fifty usernames into the field.

Local Groups - To modify the list of local group objects associated with a policy, select the *Local Groups* radio button to display the *Local Groups* input field then use the drop-down boxes in the *Local Group* column to add a maximum of fifty groups to the input field, three at a time. Click the *Save and Redisplay* button for more empty drop-down boxes.

Note: Refer to the LOCAL Groups section in Chapter 5 for instructions on how to configure *Local Groups* for use with policies.

IP Addresses - To modify the list of IP address objects associated with a policy, select the *IP Addresses – Workstation/Network* radio button to display the *IP Address* and *IP Mask* input fields. Enter IP addresses and range masks into the appropriate fields, a maximum of fifty pairs, three at a time. Click the *Save and Redisplay* button for more empty fields.

Configuring NT Security Groups Directory Objects

Important: The *ContentKeeper Agent* must be configured and running in order for the NT-Security Groups directory service to work.

Note: Refer to the ContentKeeper Agent section in Chapter 5 for instructions on how to install and configure the *ContentKeeper Agent* for use with policies.

NT Usernames - To modify the list of NT username objects associated with a policy, select the *NT Usernames* radio button to display the *Usernames* input field then enter a maximum of fifty usernames into the field by clicking on the desired username in the *Select Usernames* column.

NT Groups - To modify the list of NT group objects associated with a policy, select the *NT Groups* radio button to display the *NT Security Groups* input field. Use the drop-down boxes in the *NT Security Groups* input field to add a maximum of fifty domains or user groups to the input field, three at a time. Click the *Save and Redisplay* button for more empty drop-down boxes, and to load the new domain or user group settings into the policy.

Note: Click the *View Users* hyperlink to view a list of users in the selected domain or user group.

IP Addresses - To modify the list of IP address objects associated with a policy, select the *IP Addresses – Workstation/Network* radio button to display the *IP Address* and *IP Mask* input fields. Enter IP addresses and range masks into the appropriate fields, a maximum of fifty pairs, three at a time. Click the *Save and Redisplay* button for more empty fields.

Configuring LDAP and eDirectory(NDS) Directory Objects

The procedures for configuring *LDAP Directory Objects* and *eDirectory(NDS) Directory Objects* are the same.

Important: *LDAP/eDirectory Groups* must be configured in order for the LDAP or the eDirectory(NDS) *Directory Services* to work.

Note: Refer to the LDAP/eDirectory Groups section in Chapter 5 for instructions on how to configure LDAP and Novell eDirectory connectivity for use with policies.

LDAP and eDirectory Usernames - To modify the list of *LDAP* or eDirectory username objects associated with a policy, select the *LDAP Usernames* or the *eDirectory Usernames* radio button to display the *Usernames* input field then enter a maximum of fifty usernames into the field by clicking on the desired username in the *Select Usernames* column.

LDAP and eDirectory Groups - To modify the list of *LDAP* or eDirectory group objects associated with a policy, select the *LDAP Groups* or the *eDirectory Groups* radio button to display the *Groups* input field. Use the drop-down boxes in the *LDAP or eDirectory Groups* input field to add a maximum of fifty user groups to the input field, three at a time. Click the *Save and Redisplay* button for more empty drop-down boxes, and to load the new user group settings into the policy.

Note: Click the *View Users* hyperlink to view a list of users in the selected domain or user group.

IP Addresses - To modify the list of IP address objects associated with a policy, select the *IP Addresses – Workstation/Network* radio button to display the *IP Address* and *IP Mask* input fields. Enter IP addresses and range masks into the appropriate fields, a maximum of fifty pairs, three at a time. Click the *Save and Redisplay* button for more empty fields.

5. Verify / Test the new Policy

ContentKeeper includes facilities for verifying and reporting on policies. These facilities will assist in confirming the proper functioning of policies.

Note: Refer to the Verify Policy section in Chapter 5 for an explanation of how to use the *ContentKeeper Policy Verification* facility.

Note: Refer to the Display Policies section in Chapter 5 for more information on the *ContentKeeper Policy Reports* facility.

6. Enable the Policy

The final step in creating policies is to enable them. This may be achieved through the following steps:

1. Return to the *Create and Edit Policies* menu.
2. If necessary, use the drop-down box to select the desired policy.
3. Check the *Enable Policy* check box by clicking on it.

The policy is now enabled.

The Default Policy

ContentKeeper has two special policies, the *Default Policy* and the *Global Policy*. The *Default Policy* is always enabled and has no *Directory Service* or *Directory Objects* associated with it. Any URL request is automatically matched to the *Default Policy*, unless it is matched to a *Custom Policy* as determined by *ContentKeeper Policy Logic*.

The Global Policy

The *Global* policy is an optional component of *ContentKeeper Policies*. It may be enabled or disabled depending on your organisations requirements, and is accessible from the *Create & Edit Policies* menu.

Settings within the *Global* policy will apply to, and override, all other policies with the exception of the *Default Policy*, thus enabling an administrator to affect a change on all policies without having to edit each one individually.

Configuration of the *Global Policy* is exactly the same as configuration of the *Default Policy* with the exception of the default *Blocking State*, which is *Ignore*.

When a *Blocking Type* is set to *Ignore*, no modification of settings for that *Category* will apply to any other policy.

Important: All settings within the *Global Policy* will override those of all other policies with the exception of the *Default Policy*.

Silent Mode

Use *Silent Mode* to test policies and policy configuration changes without impacting on Internet access for your organisation. By using *Silent Mode* you are able to easily and confidently tune policies to suit a specific environment or need without impacting on user performance or productivity.

Understanding Silent Mode

When ContentKeeper is operating in *Silent Mode* it will not generate any *blockpages* in response to URL requests, instead it will allow URL requests that would normally be blocked and make a *Silent Mode* blocking event entry in the *Current Blocking Activity* report.

Normal blocking event entries in the *Current Blocking Activity* report appear in a colour with an asterisk (*), red for *Block*, blue for *Authenticate* and green for *Coach*. *Silent Mode* blocking event entries in the *Current Blocking Activity* report appear without a colour or an asterisk, this makes them easily identifiable. In the example below entries 3 and 6 are *Silent Mode* blocking event entries.

Count	Hits	Category	Mode	Parent-Domain	Ip	User	Time	Policy	Method
1	1	Chatrooms	Block*	www.satanosphere.com	192.9.200.228	duncan	07-03-2004; 11:41:51	d-policy	List
2	1	Adult Content	Block*	www.mrwordsmith.com	192.9.200.228	duncan	07-03-2004; 11:42:06	d-policy	List
3	1	Adult Content	Block	www.mrwordsmith.com	192.9.200.194	administrator	07-03-2004; 12:42:20	a-policy	List
4	1	Adult Content	Block*	www.mrwordsmith.com	192.9.200.194	matthew	07-03-2004; 12:42:29	matts-policy	List
5	1	www-Email Sites	Coach*	www.hotmail.msn.com	192.9.200.245	aaron	07-03-2004; 10:31:42	aaron	List
6	1	www-Email Sites	Block	www.hotmail.com	192.9.200.245	administrator	07-03-2004; 10:30:53	a-policy	List

Configuring Silent Mode

Silent Mode may be enabled on both a global level and on a policy level. When *Silent Mode* is enabled on a global level, all policies will operate in *Silent Mode*. When *Silent Mode* is enabled on a policy level, only policies configured to do so will operate in *Silent Mode*.

To enable *Silent Mode* on a global level, select *General Parameters* from the *General Settings* menu then set the *ContentKeeper Blocking* drop-down to *Off* and click the *Save* button.

To enable *Silent Mode* on a policy level, first select *Create & Edit Policies* from the *Blocking/Reporting* menu to display the *Policy Management Table*. Next select the desired policy from the *Select Policy* drop-down and click on the *Other Rules* button. Finally select *No* from the *Generate a Blocking Page if URL Blocked* drop-down and then click the *Save and Redisplay* button.

Using Silent Mode

Silent Mode is most commonly used when ContentKeeper is first deployed or when new policies are created. The following procedure forms a guide to using *Silent Mode* when deploying ContentKeeper.

1. Enable *Silent Mode* on a global level.
2. Deploy ContentKeeper.
3. Monitor Internet usage.
4. Tune policies.
5. Enable *Blocking Mode* (disable *Silent Mode*).

Note: Refer to the Deploying ContentKeeper section in Chapter 3 for more information about deploying ContentKeeper.

Configuring URL Reclassification

Note: Refer to the URL Reclassification Settings section in Chapter 5 for more information about configuring ContentKeeper *URL Reclassification*.

Configuring Live Filtering

Note: Refer to the Live Filtering Settings section in Chapter 5 for more information about configuring ContentKeeper *Live Filtering*.

Configuration Backups

A structured backup regime is essential to providing better fault tolerance and to preventing major data loss. The following table outlines ContentKeeper Technologies recommended backup regime.

Action	Details
Perform the initial configuration of ContentKeeper.	Refer to the Initial Configuration section in this chapter for more information.
Perform a *ContentKeeper Backup*.	Performing a *ContentKeeper Backup* at this stage will allow you to revert to the initial configuration at any time should you need to.
Tune your ContentKeeper appliance configuration.	Refer to the Tuning Configuration section in this chapter for more information.
Perform a *ContentKeeper Backup*.	Performing a *ContentKeeper Backup* at this stage will allow you to restore your tuned configuration should anything happen to the ContentKeeper appliance.
Continue customisation of your ContentKeeper appliance configuration.	Over time the configuration of ContentKeeper will become more and more customised to suit the user environment.
Perform *ContentKeeper Backup*.	It is recommended practice to perform a *ContentKeeper Backup* every time a change is made to the ContentKeeper configuration.
Download a copy of the most recent *ContentKeeper Backup* and store it in a safe place.	It is recommended practice to store a copy of the most recent *ContentKeeper Backup* in a safe place; somewhere off-site from the ContentKeeper appliance is preferable. This is so that if a rebuild of ContentKeeper is required, most of the configuration data is retained.

Restoring a backup of ContentKeeper version 118.02 or earlier will overwrite the *Management Port* IP address settings. This is because in ContentKeeper versions up to 118.02 the *Management Port* IP address settings were included with the backup.

Note: Refer to the ContentKeeper Backups section in Chapter 5 for a complete list of the settings included in a *ContentKeeper Backup*.

ContentKeeper Reporting

ContentKeeper provides both real-time and historical reporting facilities, as well as multiple log file formats for compatibility with a wide range of third party log file analysis and reporting utilities.

The following real-time reports are available within ContentKeeper.

- Dynamic Activity Viewer

Note: Refer to the Dynamic Activity Viewer section in Chapter 5 for more information about the *Dynamic Activity Viewer*.

- Current Username Activity

Note: Refer to the Current Username Activity section in Chapter 5 for more information about the *Current Username Activity* report.

- Current Internet Activity

Note: Refer to the Current Internet Activity section in Chapter 5 for more information about the *Current Internet Activity* report.

- Current Blocking Activity

Note: Refer to the Current Blocking Activity section in Chapter 5 for more information about the *Current Blocking Activity* report.

The following historical reports and log files are available within ContentKeeper.

- Webalizer Reports

Note: Refer to the Webalizer Reports section in Chapter 5 for more information about *Webalizer Reports*.

- Internet Activity
- Blocked Activity
- Discarded Blocked Activity
- Coach Click-Thru Activity
- Authentication Click-Thru Activity

Note: Refer to the View/Download Report Logs section in Chapter 5 for more information about accessing ContentKeeper report logs, as well as an explanation of the available report log formats.

Two additional reporting facilities are available within ContentKeeper that combine both real-time and historical information.

- Departmental Reports

Note: Refer to the Departmental Report Setup section in Chapter 5 for more information about *Departmental Reports*.

- Advanced Reporting Module

Note: Refer to the Advanced Reporting Module section in Chapter 5 for more information about the *Advanced Reporting Module*.

Troubleshooting

The basic premise of troubleshooting any ContentKeeper issue is K.I.S.S (Keep It Super Simple). More often than not the cause of an issue is simple, such as a setting being forgotten or overlooked. Searching for complex solutions to supposedly complex problems is often more likely to waste time than do any good.

The procedures outlined in each of the sections below are of a general nature and may also be applied to other general issues of a similar type.

The topics covered in this section are as follows:

- Troubleshooting DataCenter Connectivity
- Troubleshooting the H.A.M
- Troubleshooting the Auto Installer

Troubleshooting DataCenter Connectivity

The most common causes of *DataCenter* connectivity issues are incorrect *Management Port* IP address settings, and incorrect *Management Port* proxy settings.

Note: Refer to the DataCenter Connectivity Status section in Chapter 3 for more information about how and why ContentKeeper requires connectivity to the *ContentKeeper DataCenter*, and what will happen if ContentKeeper cannot connect to the *ContentKeeper DataCenter*.

Use the following procedure to help you diagnose and correct *ContentKeeper DataCenter* connectivity issues. Follow each step until one fails, then perform the necessary corrections. If the problem has not been fixed, restart the troubleshooting process and repeat until you are able to complete all steps successfully. If the problem still persists, contact ContentKeeper technical support.

Note: Refer to the Obtaining Technical Support section in the Introduction for more information about contacting ContentKeeper technical support.

1. **Browse to the *ContentKeeper Web Interface*.**

If you are able to browse to the *Web Interface* then the *Management Port* IP address is correctly configured.

If you are unable to access the *Web Interface* then you may need to review your *Management Port* IP address settings.

Note: Refer to The ContentKeeper Setup Program section in Chapter 2 for more information about using the ContentKeeper Setup Program to reconfigure the *Management Port* IP address settings.

Alternatively you may need to review the browser configuration settings on the workstation that you are browsing from. For example, you may not have bypassed the *Management Port* IP address from your local proxy server.

Note: Refer to Connecting to the Management Port and using the Web Interface section in this chapter for more information about configuring your browser.

2. **Check the *DataCenter Connectivity Status***

Verify that there is an issue with the *DataCenter Connectivity Status* by examining the *DataCenter Connectivity Status* in the *Summary of Bridge and DataCenter Connectivity Status* table at the bottom of the *Status Information* menu.

Note: Refer to the DataCenter Connectivity Status section in Chapter 5 for more information about the *DataCenter Connectivity Status* value.

If the *DataCenter Connectivity Status* value is anything other than Okay you may have an issue with the *DataCenter Connectivity Status*. Wait for no more than ten minutes then refresh the *Status Information* menu and re-examine the *DataCenter Connectivity Status* field. ContentKeeper may have just been starting up or restarting.

If ContentKeeper does not connect to the *DataCenter* then proceed with the troubleshooting process.

3. Ensure that ContentKeeper is operating.

If ContentKeeper is not operating it will not connect to the *ContentKeeper DataCenter*. Usually if ContentKeeper is not operating you will see a message above the *Web Interface* main menu warning you of the fact.

To verify that ContentKeeper is operating, browse to the *Status Information* menu and examine the *Process Uptime* field. Unless you have manually restarted or reconfigured the ContentKeeper appliance since it was last booted, the value in the *Process Uptime* field should match that in the *Machine Uptime* field.

Note: Refer to the Status Information section in Chapter 5 for more information about using the *Current Status* menu.

If the value in the *Process Uptime* field does not match that in the *Machine Uptime* field, wait for no more than three to five minutes then refresh the *Status Information* menu and re-examine the *Process Uptime* field. ContentKeeper may have just been starting up or restarting.

Keep refreshing. If the *Process Uptime* does not increase in a steady manner or ContentKeeper does not start, restart ContentKeeper from the *Restart* menu. If this does not work, please contact ContentKeeper technical support.

Note: Refer to the Restart Menu section in Chapter 5 for more information about using the *Restart* menu.

---

4. Confirm the *Management Port* IP address settings

Confirm the IP address settings of your *Management Port* by browsing to the *Appliance Configuration Settings* menu and reviewing the information displayed there. You may need to review your *Management Port* IP address settings.

Note: Refer to the Appliance Configuration Settings section in Chapter 5 for more information about using the *Appliance Configuration Settings* menu.

Note: Refer to The ContentKeeper Setup Program section in Chapter 2 for more information about using the ContentKeeper Setup Program to reconfigure the *Management Port* IP address settings.

---

5. **Test proxy server connectivity.**

   If your ContentKeeper appliance is connecting to the *ContentKeeper DataCenter* via a proxy server, then test the connectivity between ContentKeeper and the proxy server by clicking on the *Save and Test Only* button in the *Management Port Proxy Settings* menu.

   Note: Refer to the Testing Connectivity section in Chapter 5 for more information about testing the *Management Port* proxy settings.

   You may need to reconfigure your *Management Port* proxy settings.

   Note: Refer to the Authentication Settings section in Chapter 5 for more information about using ContentKeeper with an authenticating proxy server.

6. **Ping the *ContentKeeper DataCenter***

   Check that you have connectivity with the *ContentKeeper DataCenter* by pinging *base.contentkeeper.com* from a network workstation on the same network segment as the ContentKeeper *Management Port*. If you receive no reply from *base.contentkeeper.com*, please contact ContentKeeper technical support.

Troubleshooting the H.A.M

The most common causes of *High Availability Module* issues are incorrect cabling and incorrect configuration of the *Ignore UTP Gigabit Heartbeat* parameter.

Note: Refer to the High Availability Module (H.A.M) section in Chapter 2 for more information about installing and configuring the *H.A.M*.

Use the following procedure to help you diagnose and correct *High Availability Module* issues. Follow each step until one fails, then perform the necessary corrections. If the problem has not been fixed, restart the troubleshooting process and repeat until you are able to complete all steps successfully. If the problem still persists, please contact ContentKeeper technical support.

Note: Refer to the Obtaining Technical Support section in the Introduction for more information about contacting ContentKeeper technical support.

1. **Ensure ContentKeeper has been configured to use the *H.A.M*.**

   The *H.A.M* will not switch to *Online* mode until it has been enabled within the *ContentKeeper Web Interface*. Browse to the *High Availability Module (H.A.M)* menu in the *ContentKeeper Web Interface* and ensure that the

Mode parameter is set to *On*. If not, set the mode parameter to *On* then click the *Save* button to apply the new configuration to ContentKeeper.

Note: Refer to the Mode section under the High Availability Module (H.A.M) section in Chapter 5 for more information about configuring the *H.A.M Mode* parameter.

2. Query the *H.A.M*.

The information gained by querying the *H.A.M* may indicate the cause of an issue. Query the *H.A.M* by browsing to the *High Availability Module (H.A.M)* menu in the *Web Interface* and clicking the *Query-H.A.M* button.

The result of a query will indicate the current status of the *H.A.M* as well as the bypass and online *Cause Codes*.

Note: Refer to the Cause Codes And Uptime section under the *High Availability Module (H.A.M)* section in Chapter 5 for more information about connecting the *H.A.M Serial Interface*.

If ContentKeeper does not receive a response when querying the *H.A.M*, the *H.A.M Serial Interface Cable* may not be installed correctly.

Note: Refer to the Serial Interface section under the *High Availability Module (H.A.M)* section in Chapter 2 for more information about connecting the *H.A.M Serial Interface*.

3. Ensure that the *H.A.M* is correctly cabled.

The *Internet Port* and *Enterprise LAN Port* each require different types of cable when connecting to different network devices. Using the wrong cables will prevent the H.A.M. from passing Ethernet traffic.

Note: Refer to the Identifying Cable Types section under the *High Availability Module (H.A.M)* section in Chapter 2 for more information about which cables to use when connecting the *H.A.M* ports.

Refer to the table at the end of the *Identifying Cable Types* section in Chapter 2 and check that the correct cable types have been used.

4. Is the H.A.M connected to a Gigabit network?

If the *H.A.M* is connected to a Gigabit network, the *Ignore UTP Gigabit Heartbeat* parameter must be set to *On* for the *H.A.M* to function correctly.

Browse to the *High Availability Module (H.A.M)* menu in the *ContentKeeper Web Interface* and ensure that the *Ignore UTP Gigabit Heartbeat* parameter is set to *On*. If not, set the *Ignore UTP Gigabit Heartbeat* parameter to *On* then click the *Save* button to apply the new configuration to ContentKeeper.

Note: Refer to the Ignore UTP Gigabit Heartbeat section under the *High Availability Module (H.A.M)* section in Chapter 5 for more information about configuring the *H.A.M Ignore UTP Gigabit Heartbeat* parameter.

5. Ensure the Bridge Ports have been correctly configured.

Setting either the *Management Port* or *Bridge Port* Ethernet device settings to a setting that is incompatible with the Ethernet devices that they are connected to will cause them to loose connectivity with the network.

In the case of the *Management Port*, this will prevent you from accessing the *ContentKeeper Web Interface*. In the case of the *Bridge Ports*, this will prevent Ethernet traffic from flowing through the *ContentKeeper Bridge*, and may result in a network outage.

Incorrectly configured *Bridge Device Settings* may also prevent the *H.A.M* from switching to *Online* mode. Ensure that ContentKeeper *Bridge Device Settings* are correctly configured.

Note: Refer to the Selecting Bridge Device Settings section in Chapter 5 for more information about configuring ContentKeeper *Bridge Device Settings*.

Troubleshooting the Auto Installer

The most common causes of *Auto Installer* issues are unsupported hardware and unsupported PS/2 keyboards.

Note: Refer to the Using the ContentKeeper Auto Installer section in Chapter 2 for instructions on how to use the *ContentKeeper Auto Installer*.

Use the following procedures to help you diagnose and correct *ContentKeeper Auto Installer* issues. Follow each step until one fails, then perform the necessary corrections. If the problem has not been fixed, restart the troubleshooting process and repeat until you are able to complete all steps successfully. If the problem still persists, contact ContentKeeper technical support.

Note: Refer to the Obtaining Technical Support section in the Introduction for more information about contacting ContentKeeper technical support.

1. Unsupported Hardware

The following conditions are indicative of unsupported hardware.

1. The *Auto Installer* fails with a storage specific error after you have typed *install* at the boot prompt and the graphical phase of the installation has just started.

2. The *Auto Installer* completes successfully but ContentKeeper will not start after the reboot.

3. In the final phase of the installation, ContentKeeper setup fails with network interface specific errors.

If any of the above conditions arise during use of the *Auto Installer*, this may indicate that there is unsupported hardware in the appliance on which you are trying to install ContentKeeper. Please contact ContentKeeper technical support for further assistance.

2. Unsupported PS/2 keyboards.

Use the following procedures if you are using a PS/2 keyboard with the *Auto Installer*, but get no response from the keyboard.

a. Attach a PS/2 mouse to the appliance, then reboot and try again.
b. Enable *USB Keyboard Support* in the appliances BIOS, attach a USB keyboard to the appliance, then reboot and try again.

If you are still unable to make a keyboard work with the Auto Installer, please contact ContentKeeper technical support for further assistance.

Rebuilding a ContentKeeper Appliance

Rebuilding a ContentKeeper appliance is rarely necessary and should only be performed as a last resort when your ContentKeeper appliance has suffered irreparable file system damage.

If possible, you should contact ContentKeeper technical support before committing to rebuilding the appliance, as they may be able to assist you to recover the damaged appliance.

If you wish to restore your ContentKeeper appliance to factory settings, you may be able to do so by restoring the *Default-Setup-At-Installation* backup.

Important: Refer to the Default-Setup-At-Installation section in Chapter 5 for more information about using the *Default-Setup-At-Installation* backup.

How To Rebuild a ContentKeeper Appliance in 15 Minutes

Using the *ContentKeeper Auto Installer* and an up to date ContentKeeper configuration backup it is possible to completely rebuild a ContentKeeper appliance in a very short period of time, approximately fifteen minutes if you meet the necessary requirements.

To rebuild a ContentKeeper appliance in fifteen minutes, you must first meet the following requirements:

- **A recent copy of the *ContentKeeper Auto Installer* CD.**

  You will need the *ContentKeeper Auto Installer* to rebuild the ContentKeeper appliance.

  Note: Refer to the Obtaining Evaluation Software section in the Introduction for more information on obtaining the *ContentKeeper Auto Installer*.

- ***Video Console* access to your ContentKeeper appliance.**

  You will need video console access to the ContentKeeper appliance, i.e. monitor and keyboard, to use the *ContentKeeper Auto Installer*.

  Note:

- **The IP address settings of the Management Port.**

  You will need the IP address settings of the *Management Port* to reconfigure the *Management Port* during the ContentKeeper installation.

  Note: Refer to the Appliance Configuration Settings section in Chapter 5 for more information about obtaining the *Management Port* IP address settings.

- **An up to date ContentKeeper configuration backup.**

  You will need the ContentKeeper configuration backup to restore your configuration settings to the ContentKeeper appliance. If you do not have an up to date ContentKeeper configuration backup you may still proceed with an older backup, but you may loose some configuration settings in which case you will be forced to restore the lost setting in some other manner, such as remembering them.

  Note: Refer to the ContentKeeper Backups section in Chapter 5 for more information about creating and managing *ContentKeeper Backups*.

Once you have met the above requirements, use the following procedure to rebuild the ContentKeeper appliance.

Important! This rebuild procedure will result in the loss of all data on the ContentKeeper appliance, including configuration information and log files. Only rebuild your ContentKeeper appliance as a last resort.

1. Boot the ContentKeeper appliance with the *ContentKeeper Auto Installer* and follow the prompts to install ContentKeeper and reconfigure the *Management Port*.

Note: Refer to the Installing ContentKeeper section in Chapter 2 for instructions on using the *ContentKeeper Auto Installer*.

2. Browse to the *ContentKeeper Backups* menu in the *Web Interface* then upload and restore your configuration backup.

3. Confirm ContentKeeper is functioning correctly:
   - Monitor the ContentKeeper appliance and ensure that it connects to the *ContentKeeper DataCenter*.
   - Monitor the *Current Internet Activity* and ensure that traffic flowing through ContentKeeper is being logged.
   - Monitor the *Current Blocking Activity* and ensure that traffic being blocked by ContentKeeper is being logged.

Getting more help (technical support)

Note: Refer to the Obtaining Technical Support section in the Introduction for more information about contacting ContentKeeper technical support.

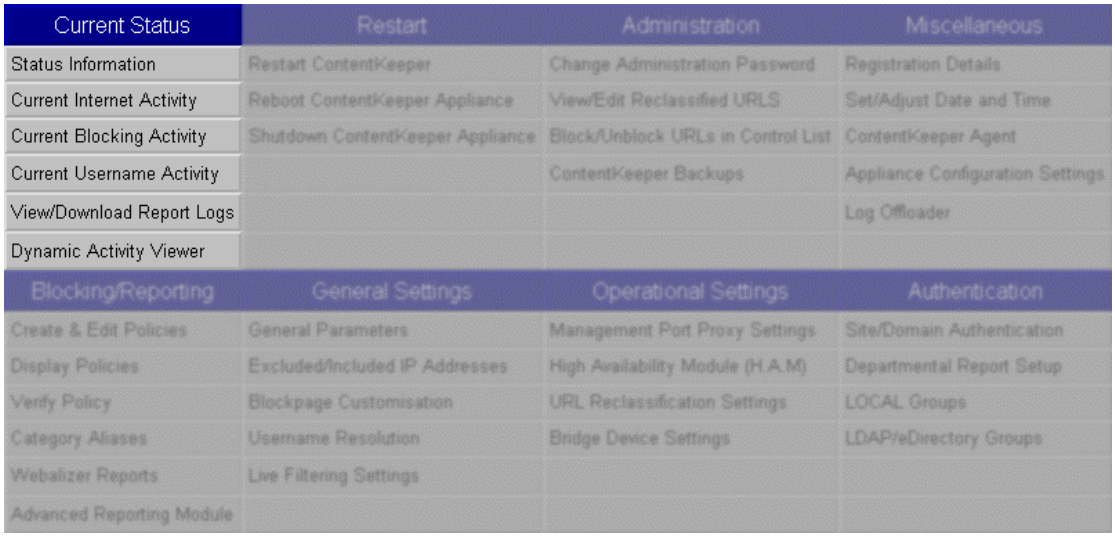
Chapter 5

Configuring ContentKeeper

Chapter 5, *Configuring ContentKeeper*, consists of a walk-thru of each of the menus of the *ContentKeeper Web Interface* and a detailed and technical description of each of ContentKeepers features and how they may be configured. This section is largely a reference section for the remainder of the Administration Guide as the information and instructions contained within are very specific. On the whole, management practices are not described here, they are described in Chapter 4. This section will contain cross-referencing to other relevant sections within the Administration Guide.

Current Status Menu

The items in the *Current Status* menu allow you to review the status of the ContentKeeper Appliance as well as current and historical access and blocking reports.



Status Information

Main Menu – Current Status → Status Information

The *Status Information* screen contains data gained from taking a snap shot of the ContentKeeper Appliance. The following information may be found in the *Current Status* screen:

- The current date and time settings of the ContentKeeper Appliance.
- The ContentKeeper *Version Number* and *Version Date.*
- The ContentKeeper Appliance *Hostname.*
- The IP and MAC addresses of the *Management Port.*
- The *High Availability Module* status.
- Your registration and license contact details.
- The Appliance *Machine Uptime* and the ContentKeeper *Process Uptime*.
- The Installed *Memory* and *Swap* file space.
- The amount of *Memory* and *Swap* file space currently being used.
- A snapshot of the network traffic traversing the *Bridge Ports* in both *Packets* and *Bytes*.
- The *Bridge Ports* Ethernet Link, Speed and Duplex status.
- The *Bridge Traffic Status* and the *DataCenter Connectivity Status*.
- The *Time Since Last Contact* and *Time To Next Contact* with the ContentKeeper DataCenter.

Version Number:	**12103**	Version Date:	**27-Feb-2004**
Hostname:	**contentkeeper**	IP/Mac Address:	**192.9.200.81 / 0010F30108A7**
Mode : **Online** Internet : **On** Lan : **On** Bridge 1 : **On** Bridge 2 : **On**			
Reg. ID:	**61-02-11246**	RX bytes (eth1):	**127 Kbits/sec**
Company:	**ContentKeeper Technologies**	RX packets (eth1):	**38 Packets/sec**
Install Date:	**29-Feb-2004**	RX bytes (eth2):	**78 Kbits/sec**
		RX packets (eth2):	**26 Packets/sec**
Contacts:-			
Technical:	**Matthew Richards**	Mem/Swap Install:	**999.4 Mb / 1992.4 Mb**
Billing:	**Matthew Richards**	Mem/Swap Usage:	**298.5 Mb / 0.0 Mb**
Address:	**218 Northbourne Ave.**	CPU Load:	**0.07**
	Braddon	DB-Status:	**100.0%**
	Canberra	Queued Connections:	**0**
	ACT,2612	Machine Uptime	**1 Days, 19:08:36**
	Australia	Process Uptime	**0 Days, 00:05:22**
Phone	**+61-02-62614950**	License type:	**Evaluation**
Fax	**+61-02-62579801**	Days license left:	**15 Day(s)**

Summary of Bridge and Datacenter Connectivity Status

Bridge Ports Status	**Port:eth1|eth2, Link: Y|Y, Autoneg: Y|Y, Speed: Auto|Auto**		
Bridge Traffic Status	**Okay**	Datacenter Connectivity Status	**Okay**
Time Since Last Contact	**0 Days, 00:00:55**	Time to Next Contact	**0 Days, 00:00:05**

High Availability Module Status

The *High Availability Module* status is indicated within the *Status Information* screen. The *High Availability Module* status may be found towards the top of the screen and will look similar to the following line:

Mode : **Online** Internet : **On** LAN : **On** Bridge 1 : **On** Bridge 2 : **On**

Mode

Mode refers to the current mode of operation of the *H.A.M*, and will be either ***Online*** or ***Bypass***.

Internet, LAN, Bridge1, Bridge2

Internet, LAN, Bridge1, Bridge2 refer to the link status, also known as connection status, of each port respectively. ***On*** indicates that there is connectivity through that particular port and ***Off*** indicates that there is not connectivity through that particular port.

Note: Refer to the High Availability Module (H.A.M) section in this chapter for more information.

Bridge Port Status

The *Bridge Port Status* is located within the *Summary of Bridge and DataCenter Connectivity Status* table at the bottom of the screen, and displays the *Bridge Ports* along with their associated Ethernet settings in the following order:

{*Bridge-Port-Interface-1}|{Bridge-Port-Interface-2}*

Bridge Ports Status	**Port:eth0|eth2, Link: Y|Y, Autoneg: Y|Y, Speed: Auto|Auto**

Port

The two Ethernet interfaces that form the *Bridge Ports* are displayed next to the *Port* descriptor.

Link

The current link status of the *Bridge Ports* is displayed next to the *Link* descriptor. A *Y* indicates that the port has established a link with its link partner. An *N* indicates that the port has not established a link with its link partner.

Note: The term *Link Partner* refers to the network interface that any given network interface is connected to. An example of two link partners may be Bridge Port 1 → A Switch Port.

Autoneg

The current auto-negotiate status of the *Bridge Ports* is displayed next to the *Autoneg* descriptor. A *Y* indicates that the port has auto-negotiate mode enabled. An *N* indicates that the port does not have auto-negotiate mode enabled.

Speed

The current speed and duplex of the *Bridge Ports* is displayed next to the *Speed* descriptor. The following table shows the complete meaning of each value that may be displayed here.

Value	Speed	Duplex
Auto	Auto-Negotiate	Auto-Negotiate
1000Mb/s-Full	1000Mbps	Full Duplex
100baseTx-FD	100Mbps	Full Duplex
100baseTx-HD	100Mbps	Half Duplex
10baseT-FD	10Mbps	Full Duplex
10baseT-FD	10Mbps	Half Duplex

Note: Refer to the Bridge Device Settings section in this chapter for information on manually specifying, or forcing, the *Bridge Port* and *Management Port* speed and duplex settings.

Inverse Video Mode

The *Bridge Port Status* is displayed in inverse video mode when there is a problem with the *Bridge Ports*.

Note: Refer to Chapter 4 for information on Troubleshooting.

Bridge Traffic Status

The *Bridge Traffic Status* is located within the *Summary of Bridge and DataCenter Connectivity Status* table at the bottom of the screen. There are two values that may be displayed alongside the *Bridge Traffic Status* descriptor. These values are:

- **Okay** – A value of *Okay* indicates that there is traffic passing through the bridge as per normal.
- **No Traffic** – A value of *No Traffic* indicates that there is no traffic passing through the bridge.

Note: Refer to Chapter 4 for information on Troubleshooting.

DataCenter Connectivity Status

The *Bridge Traffic Status* is located within the *Summary of Bridge and DataCenter Connectivity Status* table at the bottom of the screen. There are three values that may be displayed alongside the *DataCenter Connectivity Status* descriptor. These values are:

- **Okay** – A value of *Okay* indicates that the ContentKeeper appliance is in contact with the *ContentKeeper DataCenter*.
- **Connecting** – A value of *Connecting* indicates that the ContentKeeper appliance is attempting to establish communication with the *ContentKeeper DataCenter*.

Note: Refer to Chapter 4 for information on Troubleshooting.

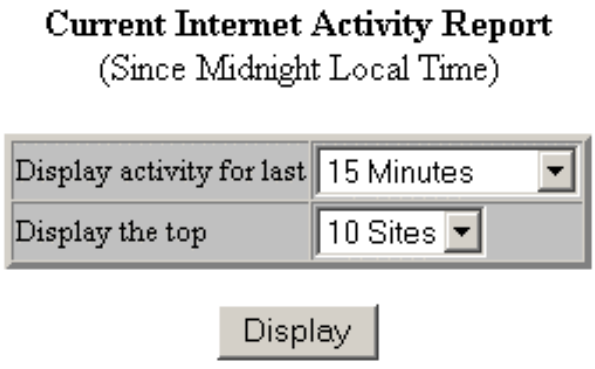
Current Internet Activity

Main Menu → Current Status → Current Internet Activity

Select *Current Internet Activity* from the *Current Status* menu to view a list of Internet sites that ContentKeeper allowed access to within the specified time frame. The *Current Internet Activity* menu will display today's Internet activity only. *Current Internet Activity* reports are generated from the ContentKeeper log files.

Note: Internet activity prior to today's may be viewed within the Internet Activity log file for the appropriate date. Refer to the View/Download Report Logs section in this chapter for information on accessing ContentKeeper log files.

Note: Refer to Chapter 4 for more information on Reporting.



Display Activity For Last

This option allows you to specify the time frame for which you wish to view Internet activity. Select a time frame between the last *5 minutes* and *Since Midnight*.

Note: The Current Blocking Activity report logs are reset at 12:00am each night.

Display The Top

Use this option to specify how many of the most frequently visited Internet sites appear when the *Display* button is clicked.

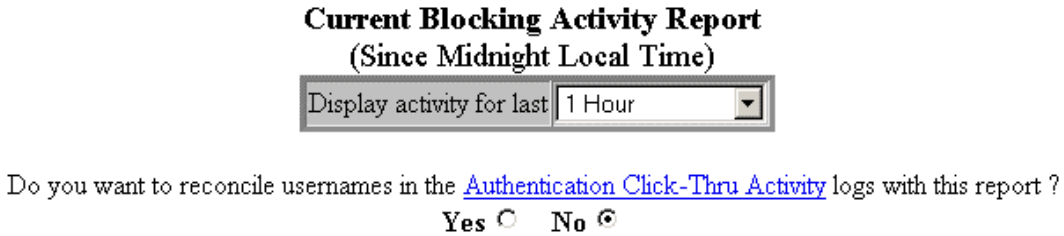
Current Blocking Activity

Main Menu – Current Status → Current Blocking Activity

Select *Current Blocking Activity* from the *Current Status* menu to view all of the URLs that have been blocked or reported by ContentKeeper within the specified time frame. The *Current Blocking Activity* menu will display today's Blocking activity only. *Current Blocking Activity* reports are generated from the ContentKeeper log files.

Note: Blocking activity prior to today's may be viewed within the Blocking Activity log file for the appropriate date. Refer to the View/Download Report Logs section in this chapter for information on accessing ContentKeeper log files.

Note: Refer to Chapter 4 for more information on Reporting.


Current Blocking Activity Report
(Since Midnight Local Time)
Display activity for last
1 Hour
Do you want to reconcile usernames in the Authentication Click-Thru Activity logs with this report ?
Yes
No

Display Activity For Last

This option allows you to specify the time frame for which you wish to view Blocking activity. Select a time frame between the last *5 minutes* and *Since Midnight*.

Note: The Current Blocking Activity report logs are reset at 12:00am each night.

Reconcile Usernames

Users who are blocked with the *Authenticate Blockpage* may supply different user credentials when authenticating to gain access to the requested URL. When users authenticate to the *Authenticate Blockpage*, an entry is made in the *Authentication Click-Thru Activity Log*.

Selecting *Yes* in reply to the *reconcile usernames* question displays the resolved username that generated the request and the supplied username that subsequently authenticated to gain access to the requested the site. A colon separates the two username entries.

For example, Matthew requested the URL www.google.com and was blocked with an *Authenticate Blockpage*. He then authenticated with a username of Mario. Selecting *No* in reply to the *reconcile usernames* question would result in the following entry in the *Current Blocking Activity Report* (Where Peru is the domain to which the user Matthew belongs).

Authenticate*	www.google.com.au	192.9.200.32	matthew/peru

Alternatively, selecting *Yes* in reply to the *reconcile usernames* question would result in a different entry in the *Current Blocking Activity Report*.

Authenticate*	www.google.com.au	192.9.200.32	matthew/peru:mario

As you can see the authenticate username has been added to the report.

Note: Refer to the Authenticate section in this chapter for more information on *Authenticate Blockpages*. Refer to the Authentication Menu section in this chapter for more information on configuring authentication for ContentKeeper.

Current Username Activity

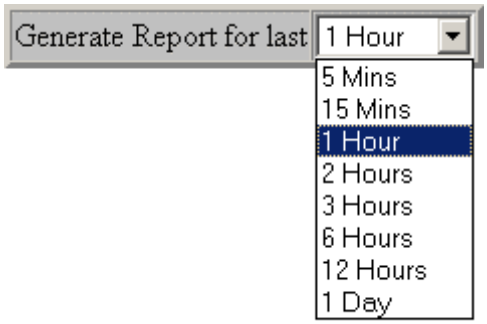
Main Menu – Current Status → Current Username Activity

Select *Current Username Activity* from the *Current Status* menu to view a report of up to one day of activity for a specified user or site (URL). *Current Username Activity* reports are generated from the ContentKeeper log files.

Note: Refer to Chapter 4 for more information on Reporting.

Generate Report for Last Dropdown Box

Use the *Generate Report for Last* dropdown box to select the time period you wish the report to cover. This time period starts the selected amount in the past and finishes in the present. You may select a period between five minutes and one day.



Value Matching

An entry in either the *Enter a Username or IP Address* or the *Enter a Partial or Complete URL* input fields may be partial or complete, as ContentKeeper will search for any value that matches the entry when generating the report.

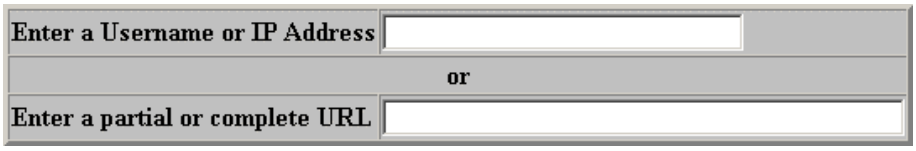
ContentKeeper will use the following logic when searching report logs (given a value of *Value*):

- ***Value*** will match ***Value***
- ***Value*** will match *anything****Value***
- ***Value*** will match ***Value****anything*
- ***Value*** will match *anything****Value****anything*

For example, entering a username of **Paul** would match **xPaul**. Additionally entering a partial IP address of **192.9.200** would match **192.9.200.88**. Similarly, entering a partial URL of **keeper.** would match **www.contentkeeper.com**.

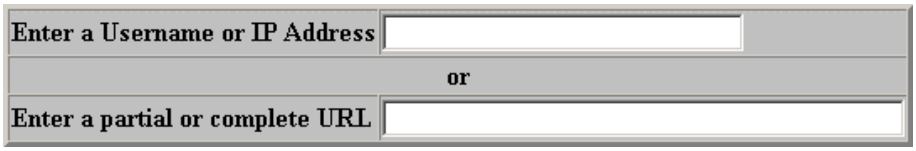
Enter a Username or IP Address

Use the *Enter a Username or IP Address* input field to specify a user on which to report in the form of a username or IP address.



Enter a Partial or Complete URL

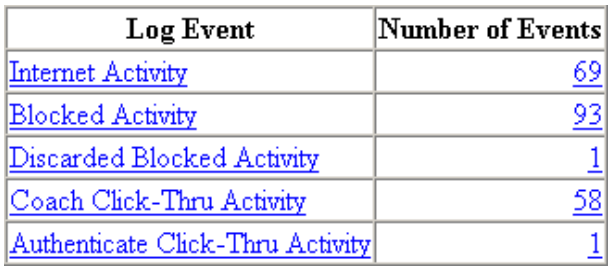
Use the *Enter a Partial or Complete URL* input field to specify a URL on which to report.



Generate Report Button

Click the *Generate Report* button to generate a report on the specified username or site (URL). A header at the top of the report screen details the report target and duration. The report itself is in the form of a table with two columns, *Log Events* and *Number of Events*.

Click on an entry in the *Log Events* column to see the associated report. Click on an entry in the *Number of Events* column to download the associated report. All reports are downloaded in CSV format.



Log Event	Number of Events
Internet Activity	69
Blocked Activity	93
Discarded Blocked Activity	1
Coach Click-Thru Activity	58
Authenticate Click-Thru Activity	1

Note: Refer to the View/Download Report Logs section in this chapter for more information on report log formats.

View / Download Report Logs

Main Menu – Current Status → View/Download Report Logs

Select *View/Download Report Logs* from the *Current Status* menu to review ContentKeeper report logs and configure the Report Log Settings. The following report logs may be viewed from this menu.

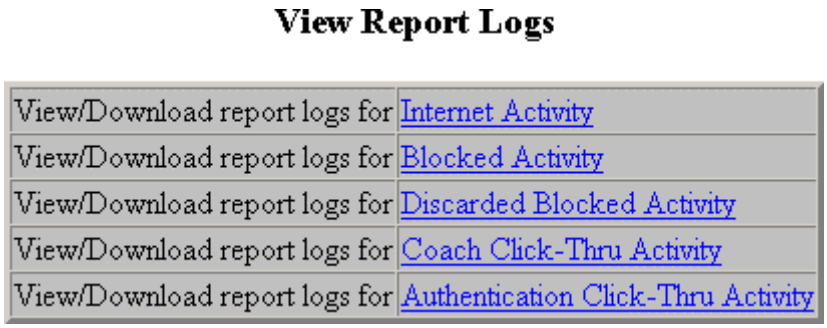
- Internet Activity
- Blocked Activity
- Discarded Blocked Activity
- Coach Click-Thru Activity
- Authentication Click-Thru Activity

All report logs are available for download in the following formats:

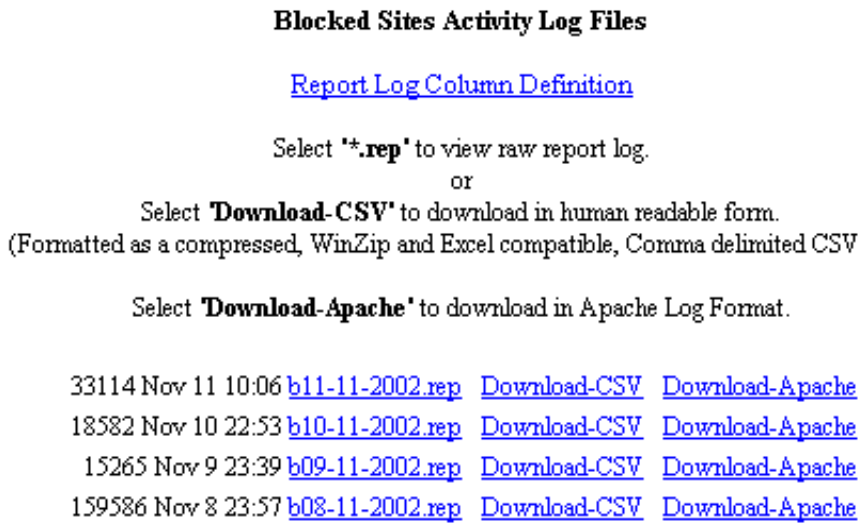
- Native ContentKeeper Format
- Comma Separated (CSV) Human Readable Format
- Apache Log Format

View Report Logs Table

Use the *View Report Logs* table to select the type of report log you wish to view or download.


View Report Logs
View/Download report logs for Internet Activity
View/Download report logs for Blocked Activity
View/Download report logs for Discarded Blocked Activity
View/Download report logs for Coach Click-Thru Activity
View/Download report logs for Authentication Click-Thru Activity

After selecting a report log type from the table at the top of the screen, a list of stored logs sorted by date will appear. Select the date for which you would like to view a log.



Blocked Sites Activity Log Files

Report Log Column Definition

Select **'*.rep'** to view raw report log.
or
Select **'Download-CSV'** to download in human readable form.
(Formatted as a compressed, WinZip and Excel compatible, Comma delimited CSV file.)

Select **'Download-Apache'** to download in Apache Log Format.

33114 Nov 11 10:06 b11-11-2002.rep Download-CSV Download-Apache
18582 Nov 10 22:53 b10-11-2002.rep Download-CSV Download-Apache
15265 Nov 9 23:39 b09-11-2002.rep Download-CSV Download-Apache
159586 Nov 8 23:57 b08-11-2002.rep Download-CSV Download-Apache

Log files are available in three different formats for compatibility with a wide range of log analysis tools, and for a greater ease of use. Simply click on the appropriate hyperlink and choose a destination to download a log file (with the exception of the ContentKeeper Native Format, see note below). The log file will be generated and the user will be prompted to continue with the download. Once downloaded, the file need only be uncompressed with a utility such as WinZip™ and the log may be viewed.

Note: To download *ContentKeeper Native Format* log files, right-click on the file name and choose *Save As*. Then proceed with the download.

Use the following information, presented in point form, to assist you in deciding which log file format will best suit your needs:

- *ContentKeeper Native Format* – By default, ContentKeeper generates all log files in this format. ContentKeeper Native Format is compatible with many Linux based log analysis tools, e.g. Webalizer

- *CSV Human Readable Format* – This format is similar to the format of the *Blocking Activity* reports. A log file downloaded in this format, once uncompressed, is compatible with most Spread Sheet applications, E.g. Microsoft Excel™. All log files of this format are comma delimited text files

- Apache Log Format – This log file format is based on the Apache Web server log file format. It is compatible with any standard web server log analysis tool. Refer to http://www.apache.org

Report Log Column Definition Table

Refer to this table, available at the top of each report log screen, for a definition of the data in each column of the report log. Usually a comma separates each column within a report log.

Block Activity
Report Log Column Definition

Column	Name	Description
1	Time	Time record was logged. Value is seconds since epoch (1st Jan 1970).
2	Category Index	1 to 32 are Standard Categories. Other values imply blocked by administrator.
3	Block Mode	2-Block, 3-Coach, 4-Authenticate.
4	Url	URL that was blocked.
5	IP Address	IP Address of workstation that block occured on.
6	Resolved IP Address	This could be 'null', 'DNS name Lookup', 'BIOS name Lookup' or 'UserName'
7	Policy	Policy and Directory Service Details
8	Method	1=Live Blocked, 2=Control List Blocked, 3=Custom or File Type Blocked

Report Log Settings

Select *View/Download Report Logs* from the *Current Status* menu to access the *Report Log Settings* tables. Use the *Report Log Settings* tables to configure the *Log File Age*. The *Log File Age* dictates how long ContentKeeper will store report log files. Statistics of the number and size of report logs and hard disk space are presented in table form. ContentKeeper uses the currently available data to project future log file space requirements and then recommends a log file age based upon that projection.

Disk Size

Size of data partition at installation	34.7 Gb
Amount of data partition currently avaliable	31.9 Gb
Amount of data partition currently used	1.1 Gb
Percent of data partition currently used	4%

Number of Log Files Generated

Number of **Internet Activity Log** files generated	144
Number of **Blocking Activity Log** files generated	136
Number of **Discarded Blocking Activity Log** files generated	117
Number of **Coach Click-Thru Activity Log** files generated	121
Number of **Authentication Click-Thru Activity Log** files generated	25

Size of Log Files Generated

Size of all **Internet Activity Log** files generated	266.8 Mb
Size of all **Blocking Activity Log** files generated	12.4 Mb
Size of all **Discarded Blocking Activity Log** files generated	5.7 Mb
Size of all **Coach Click-Thru Activity Log** files generated	4.4 Mb
Size of all **Authentication Click-Thru Activity Log** files generated	0.102 Mb

Choose a *Log File Age* from the drop down box at the bottom of the screen, then click the *Save* button to apply the new configuration to ContentKeeper.

Summary

Average size of Log files generated daily	0.533 Mb
Recommended **Log File Age**	12 Months
Set new **Log File Age**	12 Months

Once log files exceed the *Log File Age* they will be deleted from the ContentKeeper Appliance.

Note: If you wish to archive log files so they are not deleted after they exceed the *Log File Age*, or if you would prefer to store the log files on another server, then refer to the Log Offloader section in this chapter.

Dynamic Activity Viewer

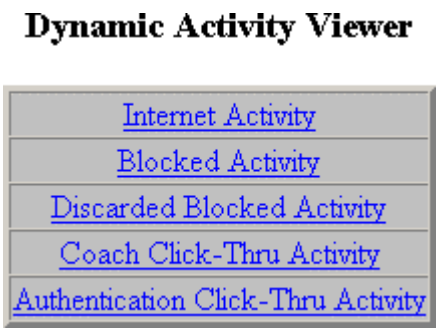
Main Menu – Current Status → Dynamic Activity Viewer

Select *Dynamic Activity Viewer* from the *Current Status* menu to view real-time *Internet Activity* and *Blocking Activity* reports. *Dynamic Activity* reports are generated in real-time from the ContentKeeper log files.

Note: Refer to the ContentKeeper Reporting section in Chapter 4 for more information on reporting.

Dynamic Activity Viewer Table

Use the *Dynamic Activity Viewer* table to select the type of *Internet Activity* or *Blocking Activity* you wish to view.



Note: Refer to the View/Download Report Logs section in this chapter for more information on report log formats.

Select the type of *Internet Activity* or *Blocking Activity* you wish to view by clicking on the appropriate hyperlink. A new browser window, containing the dynamic activity report, will automatically open.

Dynamic activity reports are generated for the current day only and will expire at midnight.

Internet Activity Viewer

The *Dynamic Internet Activity Viewer* contains a dynamically updated real-time report of the current Internet activity. A date line at the top of the report indicates the day for which the report is valid. The remainder of the report consists of a table containing the following columns:

- **Time** – The time that the URL request was made.
- **IP-Address** – The source IP address of the request.
- **Username** – The user who made the request.
- **URL** – The URL that was requested.

Live Current Internet Activity for the : 17-Feb-2004

Time	IP-Address	Username	URL
21:08:03	192.9.200.228	duncanw	24.192.90.89/.pkt
21:10:50	192.9.200.195	matthew	www.google.com
21:10:50	192.9.200.195	matthew	www.google.com.au
21:11:08	192.9.200.195	matthew	www.google.com.au
21:11:09	192.9.200.195	matthew	www.google.com.au/intl/en_au/images/logo.gif
21:11:10	192.9.200.195	matthew	www.google.com.au/intl/en_au/images/logo.gif

Blocked Activity Viewers

The *Dynamic Blocked Activity Viewers* contain a dynamically updated real-time report of the current blocked activity. All of the *Dynamic Blocked Activity Viewers* have the same format. A date line at the top of the report indicates the day for which the report is valid. The remainder of the report consists of a table containing the following columns:

- **Time** – The time that the URL request was made.
- **Category** – The *Category* to which the requested URL belongs.
- **IP-Address** – The source IP address of the request.
- **Username** – The user who made the request.
- **URL** – The URL that was requested.

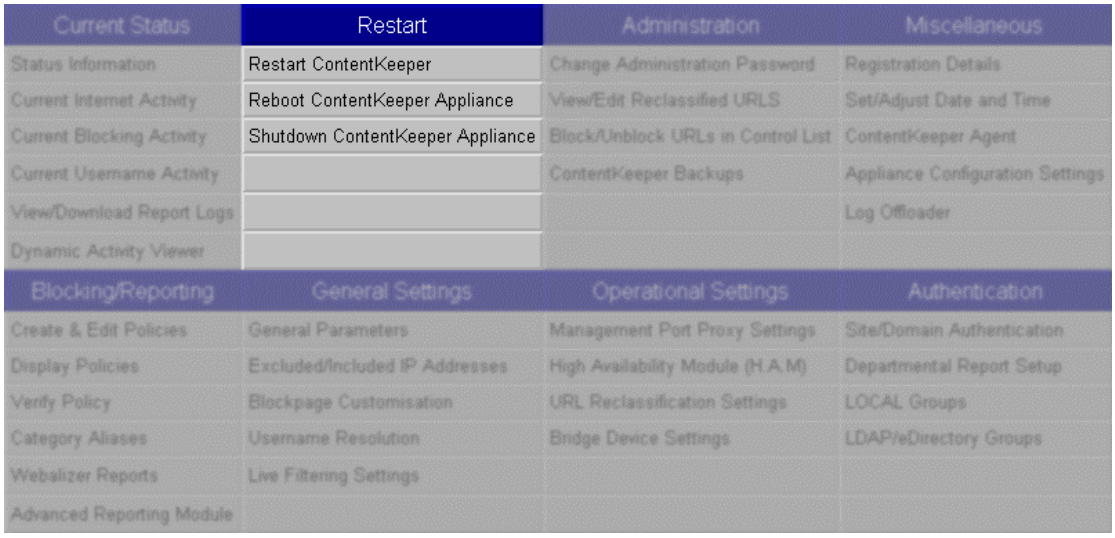
Live Current Blocking Activity for the : 17-Feb-2004

Time	Category	IP-Address	Username	URL
20:11:01	Shopping	192.9.200.172	peter	ad.au.doubleclick.net/ad/arnnet.email.com.au
21:10:47	Search Sites	192.9.200.195	administrator	www.google.com
21:28:04	Adult Content	192.9.200.15	brad	www.playboy.com
21:38:40	Music Downloads	192.9.200.80	matthew	www.mp3.com
21:42:20	Shopping	192.9.200.48	sarahh	www.shop.com
21:42:52	Music Downloads	192.9.200.80	matthew	www.mp3search.com

Note: Usernames will only appear in the *Dynamic Activity Viewers* if ContentKeeper *Username Resolution* is configured correctly. Refer to the Username Resolution section in this chapter for more information.

Restart Menu

Items in the *Restart* menu allow you to restart ContentKeeper as well as reboot and shutdown the ContentKeeper Appliance.



Restart ContentKeeper

Main Menu – Restart → Restart ContentKeeper

Select *Restart ContentKeeper* from the *Restart* menu then click the *Restart* button to stop and then immediately restart all of the ContentKeeper processes. This will cause ContentKeeper to stop filtering and stop passing Ethernet traffic for approximately 5 to 30 seconds. If the *H.A.M* is installed, it will go into *Bypass* mode during this period, allowing continued access to the Internet.

WARNING! Stopping or shutting down ContentKeeper without having the *High Availability Module* installed and activated will prevent Ethernet traffic from flowing through the bridge. This may temporarily stop your network from accessing the Internet. Refer to the High Availability Module section in this chapter for more information.

Reboot ContentKeeper Appliance

Main Menu – Restart → Reboot ContentKeeper Appliance

Select *Reboot ContentKeeper* from the *Restart* menu then click the *Reboot* button to immediately reboot the ContentKeeper server. This will cause ContentKeeper to stop filtering and stop passing Ethernet traffic for approximately 1 to 5 minutes. If the *H.A.M* is installed, it will go into *Bypass* mode during this period, allowing continued access to the Internet.

WARNING! Stopping or shutting down ContentKeeper without having the *High Availability Module* installed and activated will prevent Ethernet traffic from flowing through the bridge. This may temporarily stop your network from accessing the Internet. Refer to the High Availability Module section in this chapter for more information.

Shutdown ContentKeeper Appliance

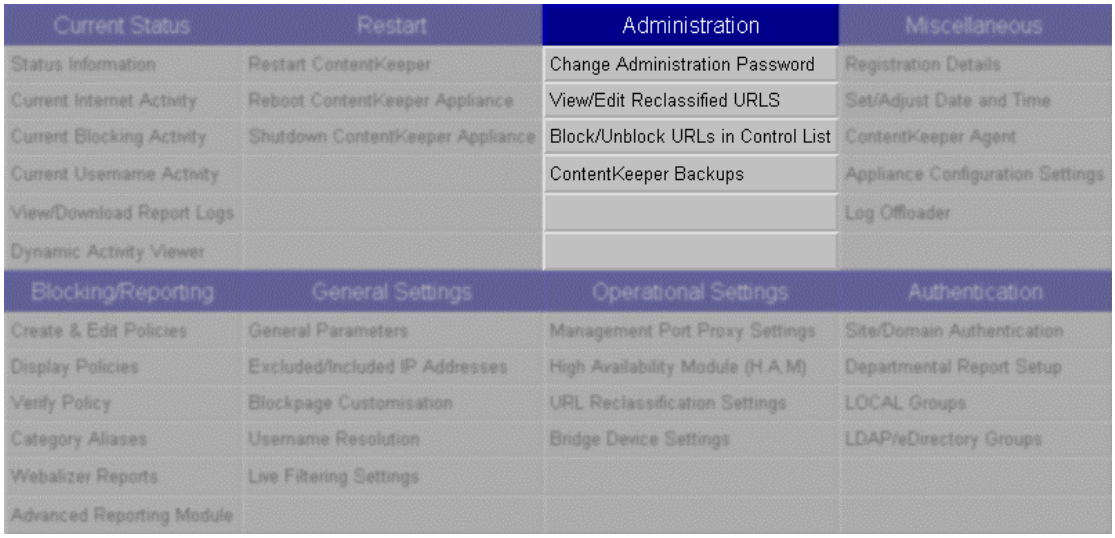
Main Menu – Restart → Shutdown ContentKeeper Appliance

Select *Shutdown ContentKeeper Appliance* from the *Restart* menu to force the server to shut down. If the H.A.M. is installed, it will go into Bypass mode during this period, allowing continued access to the Internet.

WARNING! Stopping or shutting down ContentKeeper without having the *High Availability Module* installed and activated will prevent Ethernet traffic from flowing through the bridge. This may temporarily stop your network from accessing the Internet. Refer to the High Availability Module section in this chapter for more information.

Administration Menu

Items in the *Administration* menu allow you to administer the *ContentKeeper Web Interface* login password, *Reclassified URLs* and *ContentKeeper Backups*.



Change Administration Password

Main Menu – Administration → Change Administration Password

Select *Change Administration Password* from the *Administration* menu to specify a new password for the *ContentKeeper Web Interface*. Ensure that you change the default logon password to secure your ContentKeeper server.

Note: The new password will only apply to the *ContentKeeper Web Interface* and will not affect the console (Red Hat) password.

View / Edit Reclassified URLS

Main Menu – Administration → View/Edit Reclassified URLs

Select *View/Edit Reclassified URLs* from the *Administration* menu to display, edit or revoke globally and locally reclassified URLs.

Note: It is essential that the ContentKeeper URL reclassification facility be configured correctly. URL reclassification settings determine how the local ContentKeeper server processes URL reclassification requests, as well as the degree to which your ContentKeeper site participates in the *Closed Loop Collaborative Filtering* process. Refer to the section URL Reclassification Settings in this chapter for more information.

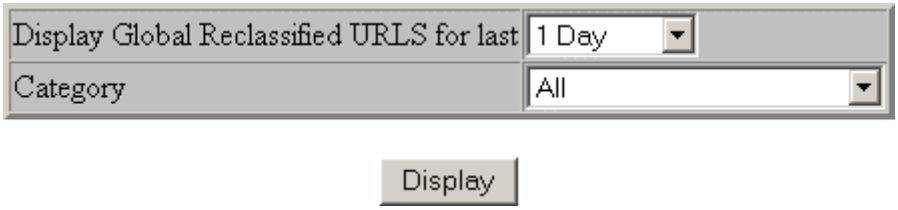
Global Reclassified URLS

Globally reclassified URLs are URLs that have been submitted for reclassification to the *ContentKeeper DataCenter*. These are URLs submitted by users via the *Submit* button on a *Blockpage*.

Use the *Display Global Reclassified URLS for Last* drop-down to specify the time frame for which you would like to view globally reclassified URLs. Select a value between one day and twelve months.

Category

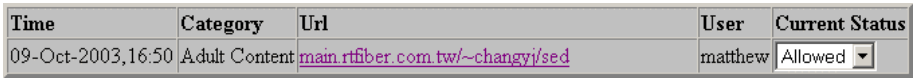
Use the *Category* drop-down to specify which categories to view reclassified URLs from. Select one of the available categories to view URLs that have been reclassified out of that category only. Select *All* to view URLs that have been reclassified out of all categories.



Display Globally Reclassified URLs

Click the *Display* button to display globally reclassified URLs according to the specified time and category settings. See below for a definition of each column.

- **Time** – This is the time and date that the URL was submitted for reclassification.
- **Category** – This is the category to which the URL formerly belonged, before being submitted for reclassification.
- **URL** – This is the URL that has been submitted for reclassification.
- **User** – This is the user that made the submission.
- **Category Status** – This column is for factory use only!



Note: A value of *Unknown* in the *User* column indicates that ContentKeeper was unable to resolve the username at the time of submission. This may indicate incorrectly configured *Username Resolution* settings. Refer to the Username Resolution section this chapter for more information.

Local URL Reclassifications

Local URL reclassifications are URLs that have been submitted for reclassification to the local ContentKeeper Appliance. These are URLs submitted by users via the *Submit* button on a *Blockpage*.

Display Local URL Reclassifications

Click the *Display Local URL Reclassifications* button to display locally reclassified URLs. See below for a definition of each column.

- **Category** – This is the category to which the URL formerly belonged, before being submitted for local reclassification.
- **URL** – This is the URL that has been submitted for local reclassification.
- **User** – This is the user that made the submission.
- **Expiry Date** – This is the date that the local reclassification of the URL is due to expire; based on URL reclassification settings.
- **Status** – The value in this column indicates the current state of the locally reclassified URL. A value of *Allowed* indicates that the time frame specified in *URL Reclassification Settings* has not elapsed since the URL was submitted. A value of *Expired* indicates that the time frame specified in *URL Reclassification Settings* has elapsed and the URL will once again be blocked under its associated category (indicated in the category column).
- **Remove Check Box** – This feature allows an administrator to revoke a locally reclassified URL from the list. This means that the next time a user browses to that URL, it will no longer be reclassified and will be blocked under its former category. Click the *Update* button after making changes to up-load the new configuration to ContentKeeper.

Category	Url	User	Expiry Date	Status	Remove
www.google.com	Search Sites	matthew	18-Feb-2004,12:03	Allowed	☐
www.acecheats.com	Game Sites	matthew	18-Feb-2004,12:04	Allowed	☐

Note: A value of *Unknown* in the *User* column indicates that ContentKeeper was unable to resolve the username at the time of submission. This may indicate incorrectly configured *Username Resolution* settings. Refer to the Username Resolution section this chapter for more information.

Block/Unblock URLs In Control List

Main Menu – Administration → Block/Unblock URLs In Control List

Select *Block/Unblock URLs in Control List* from the *Administration* menu to block or unblock, i.e. reclassify, URLs from selected categories within the ContentKeeper *Control List* (also known as the ContentKeeper *URL Database*).

Any reclassification submissions will take effect immediately in your local ContentKeeper *Control List*.

This facility forms part of the *Closed Loop Collaborative Filtering*™ system, and hence ContentKeeper will subsequently forward any URLs reclassified in this menu to the DataCenter for vetting and distribution to all other ContentKeeper Clients Worldwide.

Important: As any submissions from this menu are part of the *Closed Loop Collaborative Filtering*™ system, they will be vetted at the DataCenter and distributed back to your ContentKeeper usually within two hours. The result of this may be that a URL that you have blocked in a particular category will be unblocked from that category when it is distributed back to your ContentKeeper.

Note: You may wish to block a URL privately and not have it submitted to the DataCenter. For example, you may be a primary school that allows *Health* sites but finds certain sites are too explicit for your students and therefore would like to block those sites while still allowing access to the rest of the health sites. This may be achieved through the *Custom URLs* menu. Refer to the Custom URLs section in this chapter for more information.

Using the Block/Unblock URLs in Control List Facility

Follow the procedure below when using the *Block/Unblock URLs in Control List* facility:

1. Enter and process URLs.

   Enter the URLs you wish to add or reclassify. Refer to the Process URLs section below for more information.

2. Make and submit your URL reclassification suggestions.

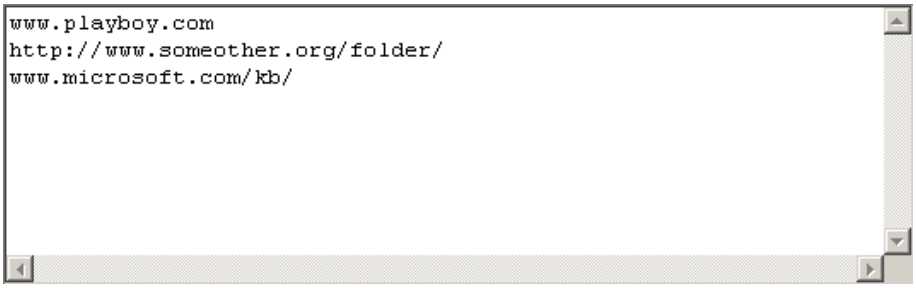
   Make your suggestions for adding or reclassifying the URLs. Refer to the Submitting Reclassification Suggestions section below for more information.

3. Verify and send your URL reclassification suggestions.

   Verify your suggestions are correct and send the URLs for reclassification. Refer to the Sending Reclassification Suggestions section below for more information.

Processing URLs

The first part of the reclassification procedure is to enter and process the URLs that you would like to reclassify (this includes adding URLs that are currently unclassified). Up to two thousand URLs may be entered into the URL input field, one per line. URLs may be entered in any form that would be accepted by your browser.



Once you have entered the URLs that you wish to reclassify, click the *Process Above Sites* button.

Submitting Reclassification Suggestions

Once you have clicked the *Process Above Sites* button, ContentKeeper will parse the URLs and redisplay them in a table along with their current classifications (if they have any).

The table containing the processed URLs has four columns. The first column contains index numbers of all the URLs entered. This column is present to allow easy counting and referencing of URLs.

The second column, *Site*, contains the actual URLs. You will notice that any URLs entered with sub-directories appear as two entries, the parent domain and the actual URL that was entered. You will also notice that some URLs appear multiple times. This is because those URLs are categorised under multiple categories and appear once per category. All of the URLs in the Site column are presented as hyperlinks for your convenience.

#	Site	Current Classification	Your Suggestion
1	www.microsoft.com	Computing/IT	
2	www.microsoft.com/kb	Computing/IT	Remove from Category
3	www.playboy.com	Adult Content	
4	www.playboy.com	Shopping	Change to - Swimsuit/Lingerie/Models
5	www.playboy.com	Entertainment	
6	www.someother.org	Unclassified	Add in - Entertainment
7	www.someother.org/folder	Unclassified	Add in - Music Downloads

The third column, *Current Classification*, contains the categories, in red, to which the URLs in the second column belong. Any URLs in the second column that are not currently classified will have a corresponding entry of *Unclassified*, in green, in the third column.

The fourth column, *Your Suggestion*, contains a drop-down for each row (or URL entry). The drop-downs are used to select an action of *Remove*, *Change* or *Add* for the corresponding URL.

Entering Suggestions

Enter reclassification suggestions by selecting the appropriate action from the drop-down in the *Your Suggestion* column. You may remove a URL from its current category, or change or add a URL to any other category. If you wish to only view the unclassified URLs, click the *Remove Classified* button.

When the *Remove Classified* button is clicked, the table will be redrawn with only the unclassified URLs.

#	Site	Current Classification	Your Suggestion
1	www.someother.org	Unclassified	Add in - Entertainment
2	www.someother.org/folder	Unclassified	Add in - Music Downloads

Once you have made all of your suggestions, click the *Submit Above Sites* button.

Sending Reclassification Suggestions

Once you have clicked the *Submit Above Sites* button, ContentKeeper will redisplay your suggestions in a new table. The table will be the same as on the previous screen with the exception of the fourth column, which will contain the *New Suggested Classification*, instead of the *Your Suggestion* drop-down.

#	Site	Current Classification	New Suggested Classification
1	www.microsoft.com/kb	Computing/IT	Remove from category **Computing/IT**
2	www.playboy.com	Shopping	Change from **Shopping** to **Swimsuit/Lingerie/Models**
3	www.someother.org	Unclassified	Add into category **Entertainment**
4	www.someother.org/folder	Unclassified	Add into category **Music Downloads**

Confirm that the reclassifications displayed are correct and click the *Send* button. The reclassification submissions will take effect immediately in your local ContentKeeper *Control List*.

Reclassification History

The *History* button allows you to view the most recent two thousand URLs that have been added or reclassified in the *Control List* via the *Block/Unblock URLs in Control List* facility.

Clicking on the *History* button will cause ContentKeeper to place a list of the most recently reclassified URLs in the URL input field. You may then click the *Process Above Sites* button to view the current classifications of the displayed URLs.

Note: If you have blocked a URL but you are still able to browse to the URL, examine ContentKeepers policy and global blocking settings. Be sure to confirm the categories under which the URL is being blocked by using the policy verify facility. Refer to the section Verifying Policies in this chapter for more information on verifying policies. Refer to the section Unique Categories in chapter 4. for more information on unique categories and their behaviour.

ContentKeeper Backups

Main Menu – Administration → ContentKeeper Backups

The *ContentKeeper Backups* facility allows an administrator to create multiple backups of ContentKeepers configuration settings. The *ContentKeeper Backups* facility also allows an administrator to download, upload and restore the various backups that have been created.

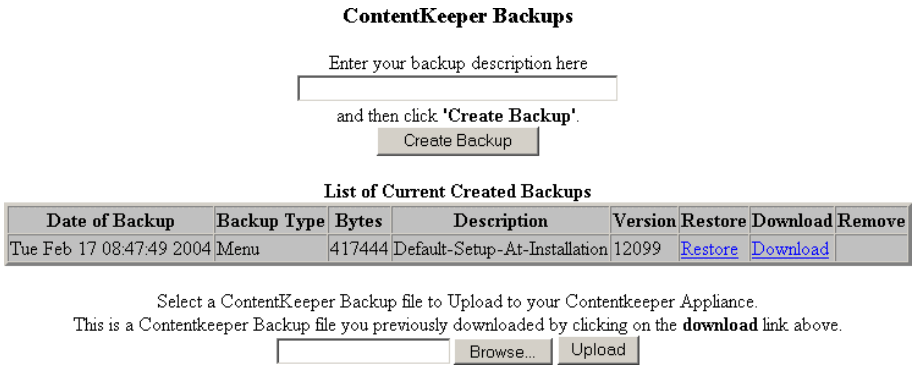
There are numerous advantages to being able to download, upload and restore backups. One of those advantages is being able to quickly recover configuration that may have taken months or years to accumulate. This is applicable in a situation where a ContentKeeper server must be rebuilt, loosing all of the data that resided on the server before the rebuild. The advantage in this situation is not just the preservation of valuable data, but also an instantaneous re-configuration of the server, which can save much time.

Select *ContentKeeper Backups* from the *Administration* menu to manage backups.

A *ContentKeeper Backup* will backup the following items:

- All ContentKeeper Menu Settings
- The Administration Password
- Registration Details
- Log Offloader Settings
- Policies
- Category States
- Custom Urls
- File-Type Settings
- Category Aliases
- General Parameters
- Excluded/Included IP Addresses
- Blockpage Customisation Configuration Data (Not the customised page itself)
- Username Resolution Settings
- Management Port Proxy Settings
- H.A.M. Settings
- URL Reclassification Settings
- Bridge Device Settings
- Site/Domain Authentication Settings
- Departmental Report Settings
- Local Group Settings
- LDAP/eDirectory Settings

Note: The *ContentKeeper Backup* does not include the ContentKeeper *Management Port* network settings or the *Ethernet Port Assignments* (i.e. which Ethernet interfaces are assigned to the *Management Port* and *Bridge Ports*). This prevents the restoration of potentially conflicting network settings to a ContentKeeper Appliance.



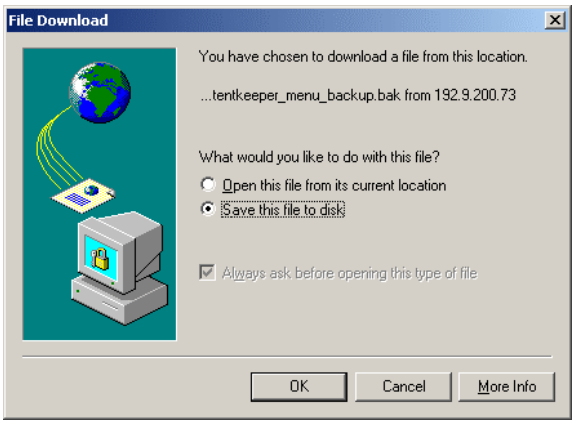
Performing Backups

To perform a backup, enter a descriptive name for the backup file into the input field at the top of the screen. This name should reflect the backup's purpose, and will allow the file to be identified at a later stage.

Next, click the *Create Backup* button. When the backup is complete the new file will appear in the *List of Current Created Backups* table.

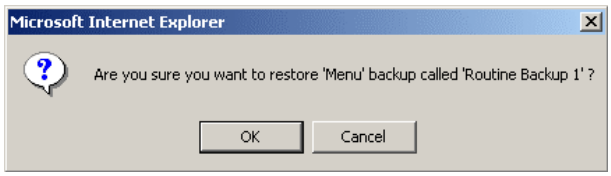
Download

Click on the *Download* hyperlink next to the desired backup file to download that file to the local computer via the browser's download function.


File Download
You have chosen to download a file from this location.
...tentkeeper_menu_backup.bak from 192.9.200.73
What would you like to do with this file?
Open this file from its current location
Save this file to disk
Always ask before opening this type of file
OK
Cancel
More Info

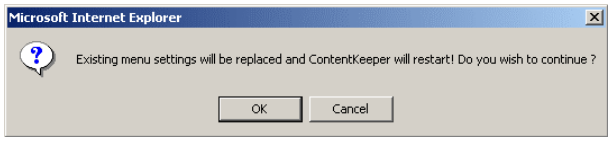
Browse | Upload

Select *Browse* and *Upload* to find a ContentKeeper backup on the local computer and to upload it to the ContentKeeper server. Once the backup is uploaded it will appear in the *List of Current Created Backups* table and may then be restored.

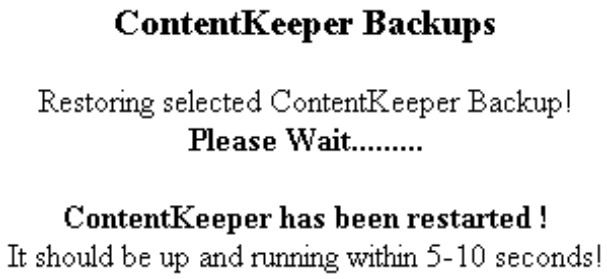


Restore

To restore a ContentKeeper backup, click the *Restore* hyperlink next to the chosen backup file. You will be prompted to confirm this action before the restore will proceed.


Microsoft Internet Explorer
Existing menu settings will be replaced and ContentKeeper will restart! Do you wish to continue ?
OK
Cancel

Warning: Restoring a backup will overwrite all of the current ContentKeeper configuration settings! Refer to the lists at the start of the *ContentKeeper Backups* section in this chapter to find out which items will be restored from a backup.


ContentKeeper Backups
Restoring selected ContentKeeper Backup!
Please Wait.....
ContentKeeper has been restarted !
It should be up and running within 5-10 seconds!

Remove

To remove a backup file from the ContentKeeper server, click on the *Remove* hyperlink. You will be prompted to confirm this action before the backup file will be deleted.

Default-Setup-At-Installation

During a new ContentKeeper installation or upon upgrade to version 120.4 or later, a factory *Default-Setup-At-Installation* backup is performed.

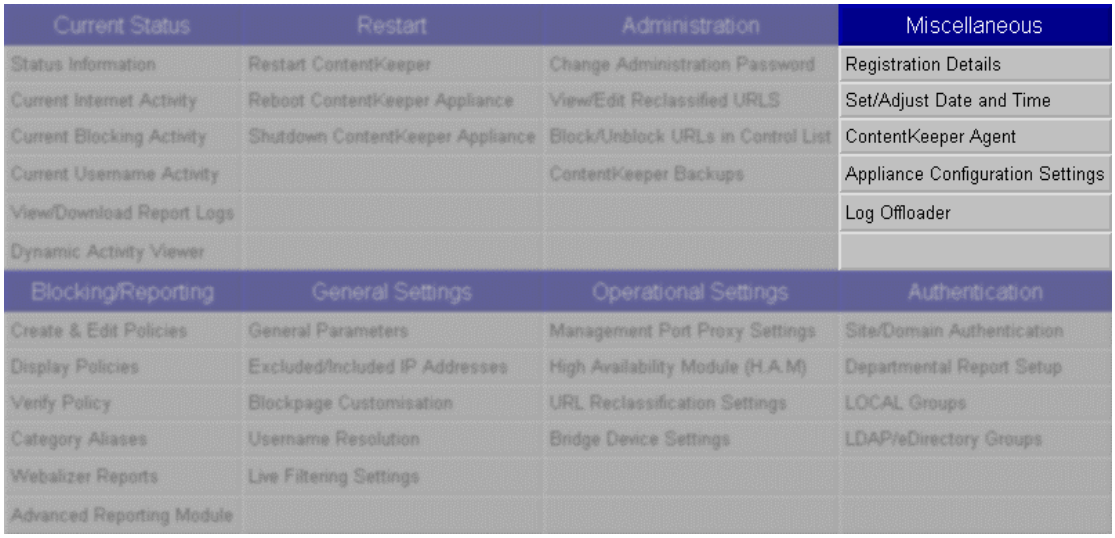
In the case of a new ContentKeeper installation, this backup contains the factory default configuration settings.

In the case of an upgrade, the current configuration is backed up instead of the factory default settings.

This backup may not be removed and is always available to return the ContentKeeper appliance to factory settings, or to the configuration at the time of the version 120.4 upgrade.

Miscellaneous Menu

Items in the *Miscellaneous* menu will allow you to change your *Registration Details* and configure the date and time on the ContentKeeper appliance, as well as download and configure the *ContentKeeper Agent*, view the *Appliance Configuration Settings*, and configure the *Log Offloader*.



Registration Details

Main Menu – Miscellaneous → Registration Details

The *Registration Details* menu allows you to change your registration, company and contact details. Select *Registration Details* from the M*iscellaneous* menu to change the following details:

- Company Name
- Address Line 1
- State
- Country Telephone Code
- Fax Number
- Billing Contact
- Address Line 2
- ZipCode
- Area Telephone Code
- Email Address
- Technical Contact
- City
- Country
- Telephone Number

Click the *Save* button after making changes to apply the new details to ContentKeeper.

Customer Registration Details

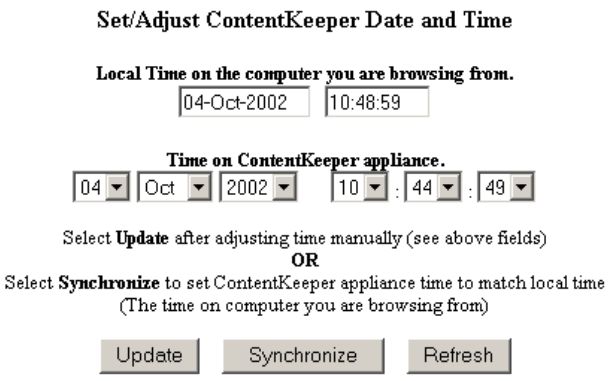
Registration Number	1-617-10181
Installation Date	05-Sep-2002
Company Name	Bill Smith
Billing Contact	Joe Bloggs
Technical Contact	Acme Company Inc.
Address 1	21 Business Road
Address 2	Malden
City	Boston
State	M.A.
ZipCode	02106
Country	USA
Country Telephone Code	1
Area Telephone Code	617
Telephone Number	555-6232
Fax Number	555-7189
Email Address	b.smith@acmecompany.com

Save

Set/Adjust Date and Time

Main Menu – Miscellaneous → Set/Adjust Date And Time

Select *Set / Adjust Date And Time* from the M*iscellaneous* menu to adjust or synchronize the time on the ContentKeeper Appliance.



Update

Click the *Update* button after adjusting any values in the date or time fields under *Time on ContentKeeper Appliance* to make the changes take effect.

Synchronize

Click the *Synchronize* button to force the time on the ContentKeeper Appliance to synchronize with the time on the computer that you are browsing from.

Refresh

Click the *Refresh* button to force your browser to refresh the current web interface screen, hence refreshing your view of the *Time on ContentKeeper Appliance*.

ContentKeeper Agent

Main Menu – Miscellaneous → ContentKeeper Agent

The *ContentKeeper Agent* is a small, simple to install application that delivers user information from a Microsoft Windows directory service to your ContentKeeper appliance. ContentKeeper applies this information to policies that have been configured to use *NT Security Groups* directory service.

The *ContentKeeper Agent* runs as a service on any Microsoft Windows NT or Windows 2000 member server or domain controller. Once installed, the *ContentKeeper Agent* periodically queries the specified domain controller for user and group information. This information is then relayed to ContentKeeper via the *ContentKeeper Agent Protocol* (CAP). By default *CAP* operates on TCP port 5555, although this may be changed to another TCP port in order to meet specific network requirements. The *ContentKeeper Agent* polls ContentKeeper every five seconds with information.

To preserve the security of the user data, all transmissions between the Agent and ContentKeeper are encrypted.

It is important to note that the *ContentKeeper Agent* initiates all communications towards the ContentKeeper appliance and that there are no listening ports opened on the Windows NT/2000 server.

Important: Before the Agent will start; it must be able to establish TCP connectivity with the ContentKeeper management port. The Agent always initiates the TCP session with ContentKeeper.

Configuring ContentKeeper To Use The Agent

Before the *ContentKeeper Agent* can be installed, ContentKeeper must be configured to listen for it. To do this, browse to the *ContentKeeper Agent* menu of the web interface and enter the configuration details.

Operation Mode

Use this option to start or stop ContentKeeper listening for the Agent. Select *On* or *Off* from the drop-down.

Install/Re-Install ContentKeeper Agent

Click the *Install/Re-Install ContentKeeper Agent* button to begin the *ContentKeeper Agent* Installation.

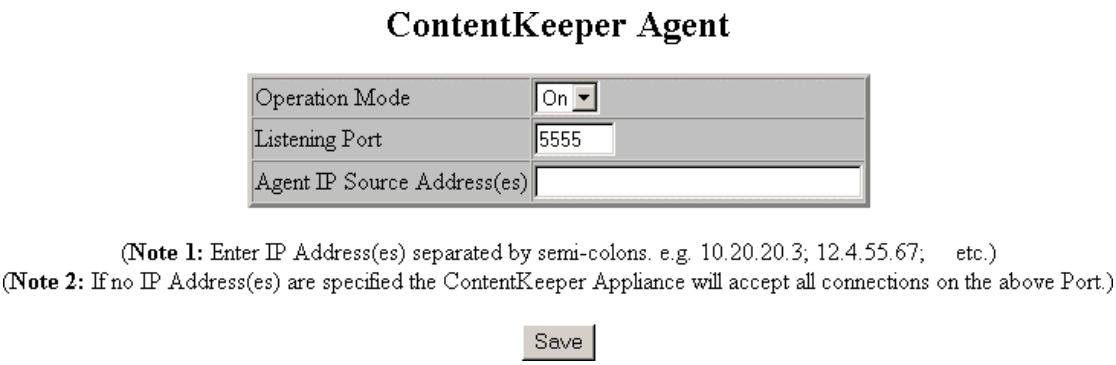
Listening Port

Specify the TCP port on which ContentKeeper will listen for the *Agent*. The default port number is 5555, which should only be changed to meet network requirements, eg. For communications through a firewall arrangement.

Agent IP Source Address(es)

If there are no IP addresses specified here, ContentKeeper will accept a connection from an *Agent* with any source IP address. Alternatively one or more IP addresses may be specified in which case, ContentKeeper will only accept connections from *Agents* with the specified IP addresses.

Note: This option is recommended for enhanced security.


ContentKeeper Agent
Operation Mode
On
Listening Port
5555
Agent IP Source Address(es)
(Note 1: Enter IP Address(es) separated by semi-colons. e.g. 10.20.20.3; 12.4.55.67; etc.)
(Note 2: If no IP Address(es) are specified the ContentKeeper Appliance will accept all connections on the above Port.)
Save

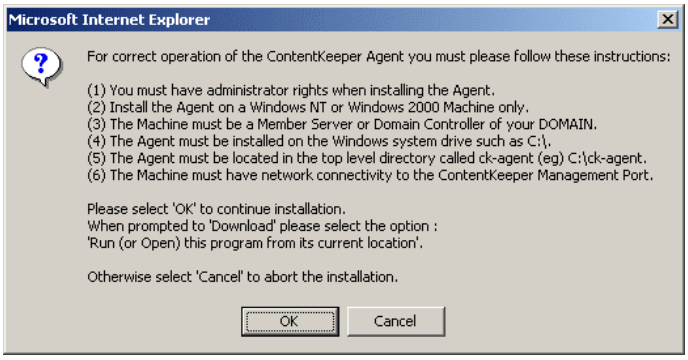
Click the *Save* button after making changes to apply the new configuration to ContentKeeper.

Installing The ContentKeeper Agent

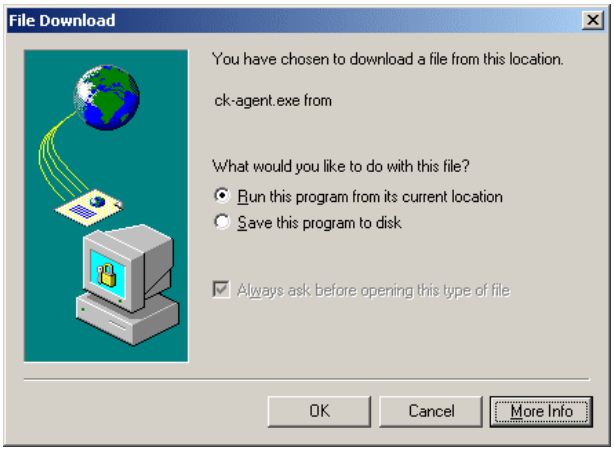
The *ContentKeeper Agent* must be installed on either a Windows NT or Windows 2000 server. The server must be a member of the domain to which the users being filtered by ContentKeeper logon. It is recommended that the following installation process be performed from the server on which the Agent is to be installed. To install the Agent, you must use an account on the target server that has administrative privileges.

1. Browse to the *Miscellaneous* menu from the ContentKeeper web interface then click on the *Install/Re-Install ContentKeeper Agent* button at the bottom of the screen.

2. A screen outlining the Agents installation requirements will appear. Ensure that all requirements are met and then click *OK* to proceed.


Microsoft Internet Explorer
For correct operation of the ContentKeeper Agent you must please follow these instructions:
(1) You must have administrator rights when installing the Agent.
(2) Install the Agent on a Windows NT or Windows 2000 Machine only.
(3) The Machine must be a Member Server or Domain Controller of your DOMAIN.
(4) The Agent must be installed on the Windows system drive such as C:\.
(5) The Agent must be located in the top level directory called ck-agent (eg) C:\ck-agent.
(6) The Machine must have network connectivity to the ContentKeeper Management Port.
Please select 'OK' to continue installation.
When prompted to 'Download' please select the option :
'Run (or Open) this program from its current location'.
Otherwise select 'Cancel' to abort the installation.
OK
Cancel

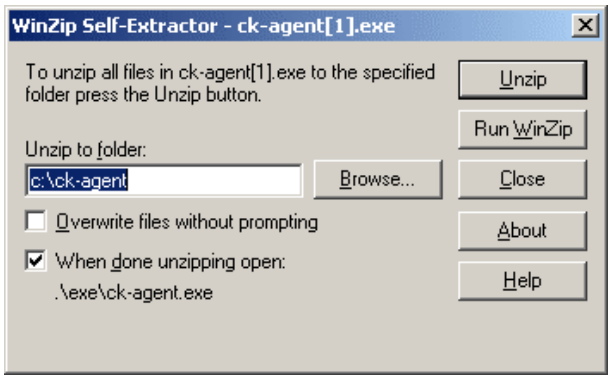
3. When the *File Download* window appears, choose *Run this program from its current location* and click *Ok* to proceed.


File Download
You have chosen to download a file from this location.
ck-agent.exe from
What would you like to do with this file?
Run this program from its current location
Save this program to disk
Always ask before opening this type of file
OK
Cancel
More Info

4. When the *Security Warning* window appears, choose *Yes* to confirm and run the *ContentKeeper Agent* installation program.

Security Warning
Do you want to install and run "ck-agent.exe from 192.9.200.68"?
The publisher cannot be determined due to the problems below:
Authenticode signature not found.
Yes
No
More Info

5. Next, the WinZip™ Self-Extractor will appear. If this installation process is not being performed from the target server, then click the browse button and select the target server. The Agent must be installed into a subdirectory of the system root drive called *ck-agent*. The *Unzip to folder* field has a default of *c:\ck-agent*. Only change this if the *ContentKeeper Agent* is not to be installed onto the local server hard drive, or if the C drive is not the system root drive.



6. Once the desired location of the *ContentKeeper Agent* files has been selected, click the *Unzip* button to extract the *ContentKeeper Agent* files. A window will appear confirming the success of the operation. Click *Ok* to launch the *Agent Monitor* and configure the *ContentKeeper Agent*.

Configuring The ContentKeeper Agent

Configuration of the *ContentKeeper Agent* is performed through the *Agent Monitor* window. The *Agent Monitor* window is automatically opened after installation completes, and may be closed at any time. Closing the *Agent Monitor* window will not stop the *ContentKeeper Agent*, which runs in the background as a Windows service. Before the Agent is started for the first time, it will need to be configured with information about the domain in which it has been installed, as well as the ContentKeeper server that it is to report to.

Domain Name – The name of the domain into which the *ContentKeeper Agent* has been installed.

Note: Refer to the NT Domain Names section under *Username Resolution* in this chapter for information on configuring how the ContentKeeper Agent enumerates usernames to ContentKeeper.

IP Address – The IP address of the target ContentKeeper Appliances *Management Port*.

Port Number – The TCP port over which the Agent will communicate with ContentKeeper. The default port number is 5555, which should only be changed to meet network requirements, eg. If this port is already being used by another network service.

Once the *ContentKeeper Agent* has been configured, click on the *Register and Start Agent* button to start the Agent. The Agent will then automatically start whenever the system boots.

Stopping And Restarting The Agent

There are two methods for stopping the Agent:

1. From the *Agent Monitor* Window, by clicking on the *Stop Agent* button.
2. From the services applet in the Windows Administrative Tools menu,
    a. Locate and highlight the service named *ContentKeeper Agent*.
    b. From the Action menu, select *Stop*.

Similar to stopping the Agent, there are two methods for starting or restarting the agent. These methods are:

1. Use the Agent Monitor Window to *Stop Ag*ent and then *Start Agent*.
2. From the services applet in the Windows Administrative Tools menu,
    c. Locate and highlight the service named "*ContentKeeper Agent*".
    d. From the Action menu, select *Restart*.

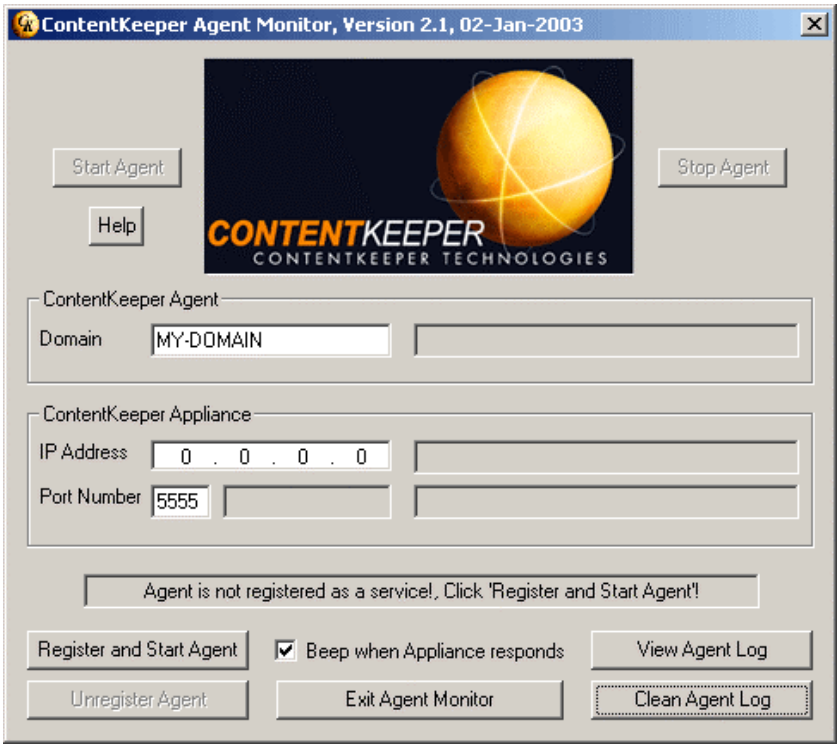
Note: The Administrative Tools menu may be found in the Windows Control Panel.

Accessing the Agent Monitor

Unless the default installation directory was changed, the *Agent Monitor* may be run from the following location:

`system-root-drive\ck-agent\exe\ckagent.exe`

Note: The system-root-drive is usually the C: drive.



The Agent Log

When you first start the *ContentKeeper Agent* an automatic connectivity test to the ContentKeeper Appliance will be run. Any errors will be displayed in the *ContentKeeper Agent* log file. If the *Agent Monitor* is active any errors will be displayed in a pop-up screen as well.

Any errors or alert messages will be appended to the *ContentKeeper Agent* log file.

To view the *ContentKeeper Agent* log file, launch the *Agent Monitor* and click the *View Agent Log* button at the bottom of the window.

To Clear the *ContentKeeper Agent* log file, launch the *Agent Monitor* and click the *Clean Agent Log* button at the bottom of the window.

The *ContentKeeper Agent* log file is automatically cleared every 24 hours.

Testing Connectivity

There are two methods for testing connectivity between the *ContentKeeper Agent* and ContentKeeper. The first method is to test connectivity from the server on which the *ContentKeeper Agent* is installed to the ContentKeeper appliance. The second method is to test that the agent is successfully communicating with the ContentKeeper applaince.

Method 1

Launch a telnet session to the ContentKeeper appliance on the *CAP* port. For example, if the ContentKeeper appliance *Management Port* has an IP address of 192.168.0.100 and is configured to listen for the *ContentKeeper Agent* on the default port 5555 the following command would be executed from the server where the agent is installed:

```
telnet 192.168.0.100 5555
```

The test may be deemed successful if the following data is returned with the response from the ContentKeeper appliance:

```
{CK-Agent}
<sRegNo>1-617-10163</sRegNo>
<sVersion>1160, 16-Aug-2002</sVersion>
<sCompany>Acme Company Inc</sCompany>
<sAction>{ntgroups-intime}</sAction>
```

The registration details will match your ContentKeeper appliance.

Method 2

Launch the *Agent Monitor* and click the *Beep when Appliance responds* check box at the bottom of the window. The local server will emit a beep (if it has an internal speaker) every five seconds to signify successful communication with the Agent. Uncheck the *Beep when Appliance responds* check box in the Agent Monitor to stop the test.

List Of Registered ContentKeeper Agents

Once one or more *ContentKeeper Agents* have been installed and configured, details of each agent may be viewed from the *ContentKeeper Web Interface* by browsing to the *ContentKeeper Agent* menu. There a table containing *ContentKeeper Agent* details will be displayed.

List of Registered ContentKeeper Agents

No.	IP Address	DNS Name	Domain	PDC	No. of Users	No. of Groups	Time Since Last Update	Current Status	Last Instruction	Force Update
1	192.9.200.221	cyber-machine.vasey-net.org	VASEY	\\VASEYWTS	11	3	0 Hrs, 17 Mins, 49 Secs	Active	Periodic	Force Update
2	192.9.200.33	home.acme-company.net	ACME	\\PROXY1	33	13	0 Hrs, 57 Mins, 33 Secs	Active	Periodic	Force Update

Refresh

Redundancy With Multiple Agents

For redundancy purposes, multiple *ContentKeeper Agents* may be installed in each domain. With multiple *ContentKeeper Agents* installed, if one of the Windows NT / 2000 servers hosting an *ContentKeeper Agent* goes offline, ContentKeeper will still be able to maintain current user and group data by using information from one of the other *ContentKeeper Agents* installed in the same domain.

Software Updates

Occasionally a new version of the *ContentKeeper Agent* will be included with a ContentKeeper update. When an update occurs, ContentKeeper will display a message at the top of the ContentKeeper Web Interface declaring the availability of a new version of the *ContentKeeper Agent*. To install the new version, follow the *ContentKeeper Agent* installation procedure outlined above and overwrite the existing *ContentKeeper Agent* program files.

The version warning on the web interface will disappear once the new version of the *ContentKeeper Agent* has been installed and is running.

Appliance Configuration Settings

Main Menu – Miscellaneous → Appliance Configuration Settings

The *Appliance Configuration Settings* menu contains a table of the ContentKeeper appliances network and Ethernet configuration data. The information displayed within this table may only be viewed and not updated from this menu.

Appliance Configuration Settings

Device name for first bridging interface	eth0
Device name for management port (Middle)	eth1
Device name for second bridging interface	eth2
Port Numbers for Filtering	3128|8080|8989
IP Address for management port	192.9.200.67
HostName management port	contentkeeper
Management port Netmask	255.255.255.0
Use Proxy	yes
Proxy IP Address	10.20.20.3
Proxy Port Number	3128
Gateway IP Address	192.9.200.100
DNS IP Address	192.9.200.100
Domain Name	domain.com.au

The following table entries are hyperlinks to other menus within the web interface. Click on a hyperlink to change its value from another menu.

- Port Numbers for Filtering
- Use Proxy
- Proxy IP Address
- Proxy Port Number

Values for the remaining entries may be modified by running the ContentKeeper setup program from the console screen.

Note: Refer to The ContentKeeper Setup Program section in Chapter 2 for information on running the ContentKeeper *Setup Program* from the *Console Screen*.

Note: It is recommended that once ContentKeeper has been installed and configured, a copy be made of the *Appliance Configuration Settings* table, either by print or electronically, as it contains all of the information required to rebuild your ContentKeeper appliance to the point where a backup may be uploaded and restored.

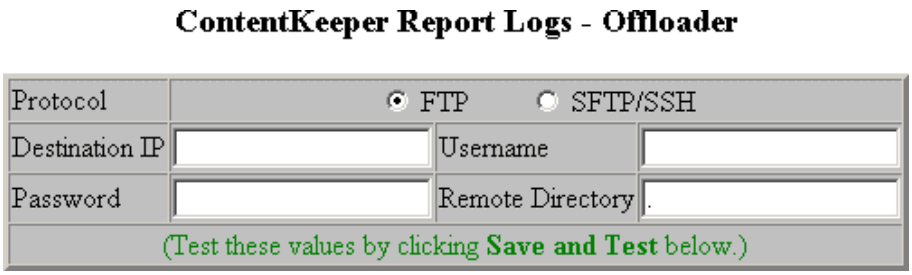
Log Offloader

Main Menu – Miscellaneous → Log Offloader

Select *Log Offloader* from the *Miscellaneous* menu to configure the ContentKeeper *Log Offloader*. The *Log Offloader* transfers ContentKeeper unencrypted log files from the ContentKeeper appliance to a specified destination via FTP or encrypted via the more secure method of SFTP/SSH.

The Offloader Table

Use the offloader table to specify the destination and method for the log transfers. Use the following sections as a guide when configuring the offloader table.



Protocol

The desired transfer method may be specified by selecting the appropriate radio button in the *Protocol* section at the top of the table. The two available options are *FTP* and *SFTP/SSH*.

Note: The destination server must be running the appropriate service, i.e. FTP or SFTP/SSH, or the *Log Offload* will fail.

Destination IP

Enter the destination for the log transfers in the form of an IP address into the *Destination IP* input field. The IP address must be specified in the form of xxx.xxx.xxx.xxx with no subnet mask.

Username

Enter the username that the *Log Offloader* will authenticate to the destination server with into the *Username* input field.

Password

Enter the password that the *Log Offloader* will authenticate to the destination server with into the *Password* input field.

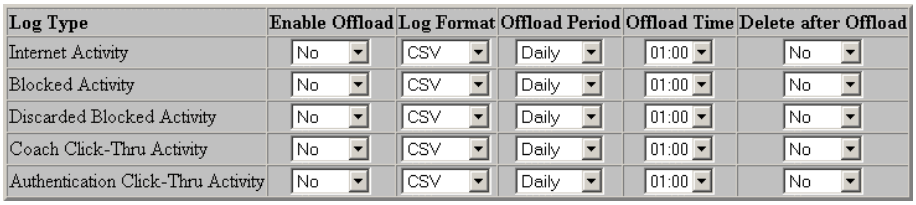
Remote Directory

Enter the remote directory that the log files will be transferred to into the *Remote Directory* input field.

Note: The remote directory must exist on the destination server or the *Log Offload* will fail.

The Log Table

Use the log table to configure which of the ContentKeeper log file types will be transferred, in what format they will be transferred and how often the transfers will take place. Use the following sections as a guide when configuring the log table.



Log Type	Enable Offload	Log Format	Offload Period	Offload Time	Delete after Offload
Internet Activity	No	CSV	Daily	01:00	No
Blocked Activity	No	CSV	Daily	01:00	No
Discarded Blocked Activity	No	CSV	Daily	01:00	No
Coach Click-Thru Activity	No	CSV	Daily	01:00	No
Authentication Click-Thru Activity	No	CSV	Daily	01:00	No

Log Type

The *Log Type* column indicates the type of ContentKeeper log file that the settings in the remaining columns will apply to.

Note: Refer to the View/Download Report Logs section in this chapter for more information on log file types.

Enable Offload

Use the *Enable Offload* drop-down to enable offloading of the respective log file type. You may specify either *On* or *Off*.

Log Format

Use the *Log Format* drop-down to specify the format that the log file will be offloaded in. The three standard ContentKeeper log formats are available, which are *RAW*, *CSV* and *Apache*.

Note: Refer to the View/Download Report Logs section in this chapter for more information on log file formats.

Offload Period

Use the *Offload Period* drop-down to specify how regularly the log files will be offloaded. You may specify *Daily*, *Weekly* or *Monthly*.

Offload Time

Use the *Offload Time* drop-down to specify which hour of the day that the log transfers should occur. Log file transfers may only be configured to take place on the hour.

Delete after Offload

Use the *Delete after Offload* drop-down to specify whether or not you would like the log files to be deleted after the transfer takes place. You may specify either *Yes* or *No*.

Zip Logs Before Transferring

You may choose to have the log files zipped (compressed) before they are transferred by selecting the appropriate radio button from the *Zip Logs Before Transferring* section, below the log table.

View Status Log

Click the *View Status Log* button to view the *Log Offloader* transfer *Status Log*. When the button is clicked the *Status Log* will be displayed in a new browser window as a table containing five columns.

Generated at: 17:10:24
Press 'refresh' on your browser for the latest information.

1	2003-12-12	15:21:36	CGI	Saved settings to configuration file.
2	2003-12-12	15:22:32	CGI	Saved settings to configuration file.
3	2003-12-12	15:22:33	CGI	FTP test failed: Couldn't connect to the IP .
4	2003-12-12	15:22:44	CGI	Saved settings to configuration file.
5	2004-01-22	08:09:05	CGI	Saved settings to configuration file.
6	2004-01-23	17:14:31	CGI	Saved settings to configuration file.
7	2004-01-23	17:14:35	CGI	SFTP test was successful.
8	2004-01-23	16:58:11	CGI	Saved settings to configuration file.
9	2004-01-23	16:58:15	CGI	SFTP test was successful.
10	2004-01-23	16:58:18	CGI	Saved settings to configuration file.
11	2004-01-23	16:58:21	Transferlog	Beginning SFTP transfer.
12	2004-01-23	16:58:21	Transferlog	Transferred the file: b23-01-2004.rep.gz.
13	2004-01-23	16:58:21	Transferlog	Finished SFTP transfer.
14	2004-01-23	16:58:21	CGI	"Save and Execute Now" is complete.

The first column contains an index of each log event for easy reference.

The second column contains the date that each log event took place.

The third column contains the time that each log event took place.

The fourth column contains a keyword indicating the type of log event. The *CGI* keyword indicates that the log event is the result of a configuration change or action initiated from the *ContentKeeper Web Interface*. The *Transferlog* indicates a log file transfer.

Save and Test

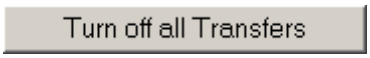
Click the *Save and Test* button to save your current *Log Offloader* configuration and perform a test connection to the target server. The result of the test will be displayed at the bottom of the offloader table, and also written to the *Status Log*.

Save and Execute Now

Click the *Save and Execute Now* button to save your current *Log Offloader* configuration and force ContentKeeper to offload the log files now instead of the configured *Offload Time*.

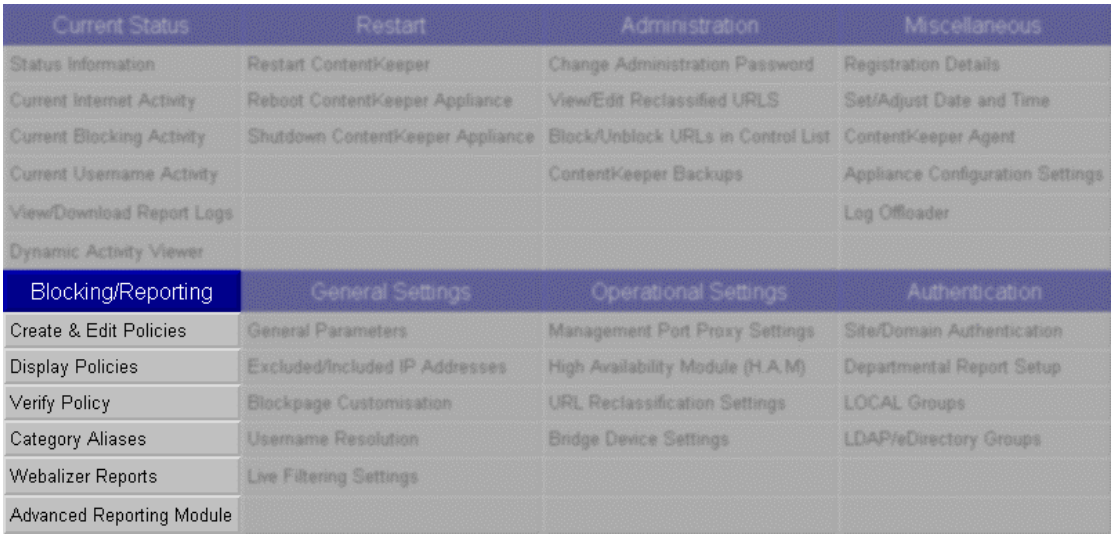
Turn off all Transfers

Click the *Turn off all Transfers* button to immediately disable all log file transfers. Log file transfers may be re-enabled in the normal fashion.



Blocking / Reporting Menu

Items in the *Blocking/Reporting* menu allow you to create, manage, display and verify *ContentKeeper Policies*. The *Blocking/Reporting* menu may also be used to configure alternative names for *ContentKeeper Categories*, known as *Category Aliases*, or configure and use the *Webalizer* reports, and access the ContentKeeper *Advanced Reporting Module*.



Create & Edit Policies

Main Menu – Blocking/Reporting → Create & Edit Policies

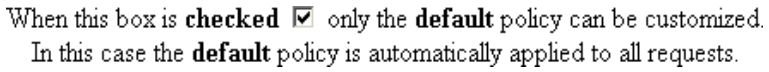
Select *Create & Edit Policies* from the *Blocking/Reporting* menu to manage all aspects of *ContentKeeper Policies*.

Note: Refer to the Configuring Policies section in Chapter 4 for a general discussion on creating *ContentKeeper Policies* as well as guidelines for creating *Custom Policies* for your organisation.

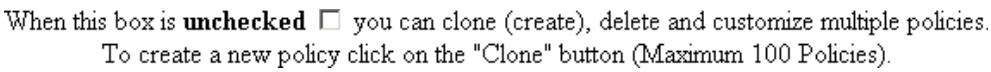
Default Only Mode

By default, ContentKeeper operates in *Default Only Mode* where only one policy is employed. This policy is known as the *Default Policy*. The *Default Policy* is always enabled and cannot be disabled, even when *Default Only Mode* has been disabled.

Note: Refer to The Default Policy section in Chapter 4 for more information on the *Default Policy*.


When this box is **checked** ☑ only the **default** policy can be customized.
In this case the **default** policy is automatically applied to all requests.

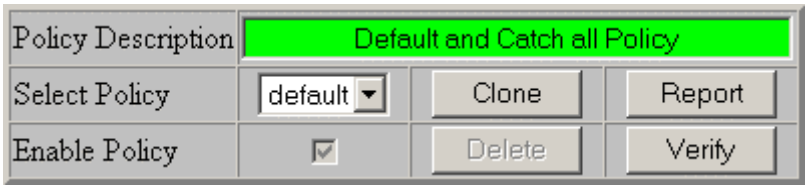
In order to create *Custom Policies*, *Default Only Mode* must be disabled. To disable *Default Only Mode*, clear the check box at the top of the *Create & Edit Policies* menu.


When this box is **unchecked** ☐ you can clone (create), delete and customize multiple policies.
To create a new policy click on the "Clone" button (Maximum 100 Policies).

Disabling *Default Only Mode* will make available previously unavailable features of the *Policy Management Table*.

Policy Cloning - Creating Custom Policies

Note: To create (clone) new *Custom Policies*, *Default Only Mode* must be disabled. Refer to the Default Only Mode section in this chapter for more information on enabling and disabling *Default Only Mode*.



To create a new *Custom Policy*, an existing policy must be cloned. A policy may be cloned by selecting the desired source policy from the *Select Policy* drop-down in the *Policy Management Table*, then clicking the *Clone* button.

Policy names may only contain the following characters, and may **not** contain spaces:

- The numbers 0 to 9
- Upper and lower case letters A to Z and a to z
- The underscore character _
- The hyphen character –

Enter a name for the new *Custom Policy* into the *Policy Name* input field, and enter a description into the *Policy Description* input field, then click the *Continue* button to complete the operation. The new *Custom Policy* will now be available from the *Select Policy* drop-down in the *Policy Management Table*.

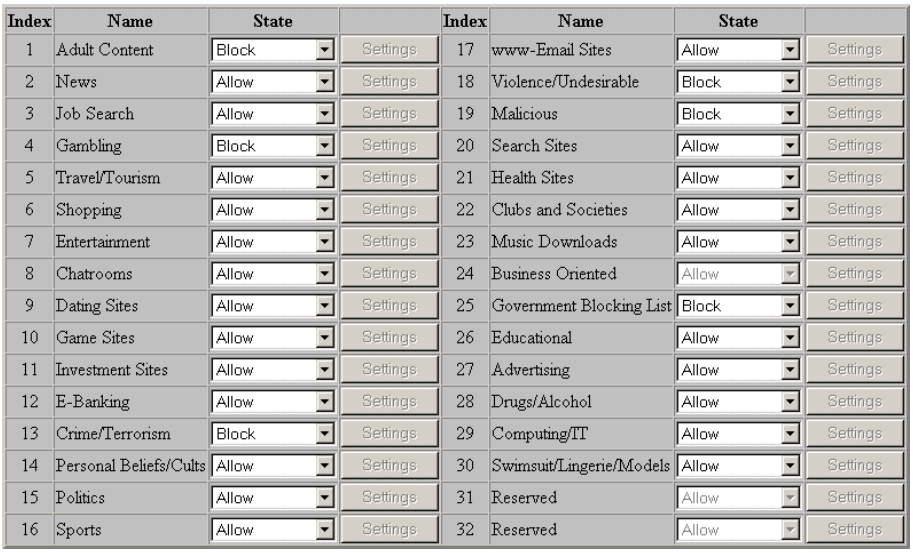
Note: Refer to the Configuring Policies section in Chapter 4 for more information on creating *Custom Policies*, including detailed procedures.

Configuring Categories

Main Menu – Blocking/Reporting → Create & Edit Policies → Categories

Click on the *Categories* button in the *Create & Edit Policies* menu to display a table listing the *ContentKeeper Categories*. Use the drop-downs in the *Categories* table to configure how ContentKeeper will filter URLs belonging to each *Category*, for the current policy.

Note: Refer to the Control List section under the Blocking Fundamentals section in Chapter 4 for an explanation of the *Category Blocking Type*.



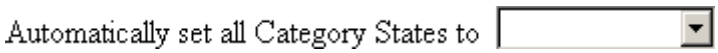
Index	Name	State		Index	Name	State	
1	Adult Content	Block	Settings	17	www-Email Sites	Allow	Settings
2	News	Allow	Settings	18	Violence/Undesirable	Block	Settings
3	Job Search	Allow	Settings	19	Malicious	Block	Settings
4	Gambling	Block	Settings	20	Search Sites	Allow	Settings
5	Travel/Tourism	Allow	Settings	21	Health Sites	Allow	Settings
6	Shopping	Allow	Settings	22	Clubs and Societies	Allow	Settings
7	Entertainment	Allow	Settings	23	Music Downloads	Allow	Settings
8	Chatrooms	Allow	Settings	24	Business Oriented	Allow	Settings
9	Dating Sites	Allow	Settings	25	Government Blocking List	Block	Settings
10	Game Sites	Allow	Settings	26	Educational	Allow	Settings
11	Investment Sites	Allow	Settings	27	Advertising	Allow	Settings
12	E-Banking	Allow	Settings	28	Drugs/Alcohol	Allow	Settings
13	Crime/Terrorism	Block	Settings	29	Computing/IT	Allow	Settings
14	Personal Beliefs/Cults	Allow	Settings	30	Swimsuit/Lingerie/Models	Allow	Settings
15	Politics	Allow	Settings	31	Reserved	Allow	Settings
16	Sports	Allow	Settings	32	Reserved	Allow	Settings

The *Categories* table consists of two blocks of four columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each *Category* for easy reference.
- **Name** – The *Name* column contains the name of each *Category*. The names displayed in the *Name* column are category aliases. Refer to the Category Aliases section in this chapter for more information on configuring *Category Aliases*.
- **State** – The *State* column contains a drop-down for each *Category*, which is used to configure the *Blocking State*. The *Blocking State* determines how ContentKeeper will filter URLs belonging to each *Category*, for the current policy. Refer to the Blocking States section in Chapter 4 for an explanation of each *Blocking State* and how it affects *ContentKeeper URL Filtering*.
- **Settings** – The *Settings* column contains a *Settings* button for each *Category*. The *Settings* button only becomes available for the *T.O.D* and *P.S.U Blocking States*. Refer to the Time Of Day and Personal Surfing Units sections in this chapter for more information on configuring the *T.O.D* and *P.S.U Blocking States*.

Note: Certain *Categories* have unique rules applied to them. Refer to the Unique Categories section in Chapter 4 for more information. Refer to the ContentKeeper Filtering Explained section in Chapter 4 for an explanation of *ContentKeeper URL Filtering*, and refer to Appendix B in Chapter 6 for a definition of each *ContentKeeper Category*.

When configuring *Category States*, you may choose to set all categories to the same state by selecting the desired state from the *Automatically set all Category States* drop-down below the *Categories* table.



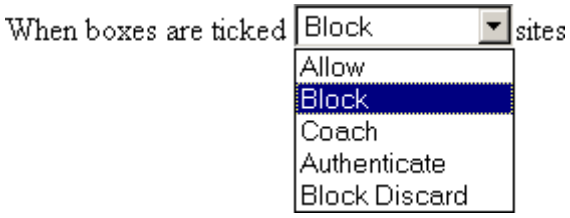
Always click the *Save and Redisplay* button after making any changes, and before leaving the *Categories* menu, this includes leaving the *Categories* menu to configure *T.O.D* or *P.S.U* settings.

Configuring Time Of Day Settings

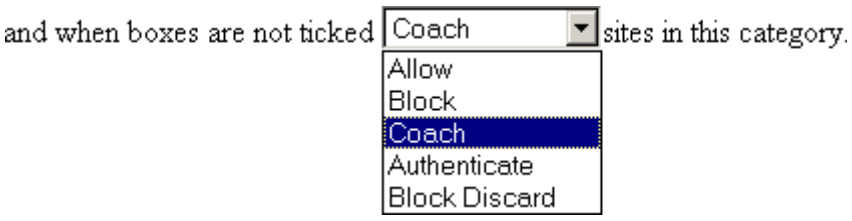
To configure the *T.O.D* settings for any *Category*, select *Time of Day* from the drop-down in the *State* column of the *Categories* table and click the *Save and Redisplay* button, then click on the associated *Settings* button. The *Time of Day Settings* screen will be displayed.

Note: Refer to the Time of Day section in Chapter 4 for an explanation of the *T.O.D Blocking State*.

Use the two drop-downs at the top of the *Time of Day Settings* screen to configure how ContentKeeper will apply the rest of the *Time of Day* settings in the *Time of Day Settings* table below.



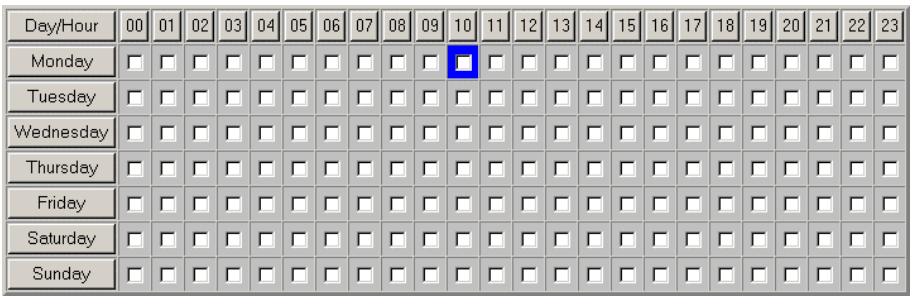
Being able to configure ContentKeeper to apply one *Blocking State* when boxes in the *Time of Day Settings* table are checked and another *Blocking State* when boxes are not checked allows for highly flexible *T.O.D* configurations.



Either of the drop-downs may be set to one of five *Blocking States*. *T.O.D* and *P.S.U Category States* may not be specified from within the *Time of Day Settings* screen.

The Time of Day Settings Table

Use the *Time of Day Settings* table to configure time frame settings. Once blocking settings have been configured (see above), proceed to configure the desired time frame settings by placing a check in the appropriate boxes.



One box represents one hour, from 0 minutes and 0 seconds to 59 minutes and 59 seconds. A time frame is specified by either checking the boxes that represent the hours within the desired time frame, or by checking the boxes that represent the hours other than the desired time frame. Several buttons have been added to this screen to make specifying a time frame easier.

Note: The blue square represents the current time according to the ContentKeeper appliance.

Click the *Save and Redisplay* button to apply your settings to ContentKeeper.

Hour Buttons

Clicking on any of the hour buttons along the top of the *Time of Day Settings* table will automatically check or clear the column of boxes below the *Hour* button. If any of the boxes in a column are checked and then the *Hour* button at the top of the column is clicked, all boxes in the column will be cleared. If no boxes in the column are checked and then the *Hour* button at the top of the column is clicked, then all boxes in the column will be checked.

Day Buttons

Clicking on any of the day buttons along the left-hand side of the *Time of Day Settings* table will automatically check or clear the row of boxes to the right of the *Day* button. If any of the boxes in a row are checked and then the *Day* button at the left of the row is clicked, then all boxes in the row will be cleared. If no boxes in the row are checked and then the *Day* button at the left of the row is clicked, then all boxes in the row will be checked.

Day/Hour Button

The *Day/Hour* button in the top left-hand corner of the *Time of Day Settings* table will automatically check or clear all of the boxes. If there are any boxes checked and the *Day/Hour* button is clicked then all boxes will be cleared. If no boxes are checked and the *Day/Hour* button is clicked then all boxes will be checked.

The following is an example of using the Time of Day feature

A corporation has an Internet Acceptable Use Policy that states, “Staff are only allowed to view shopping related Internet sites outside of work hours or during lunch hours”. The corporation’s lunch hours are between 12pm and 2pm. The following steps illustrate how an administrator could configure ContentKeeper to facilitate the corporation’s policy.

1. Log on to the *ContentKeeper Web Interface* and select *Create & edit Policies* from the *Blocking/Reporting* menu, then click the *Categories* button.

2. Select *Time of Day* from the drop-down box in the *State* column next to the *Shopping* category then click on the *Settings* button.

3. Select *Block* from the first drop-down box and select *Allow* from the second drop-down box so that the sentence reads:

   When boxes are ticked *Block* sites, and when boxes are not ticked *Allow* sites in this category

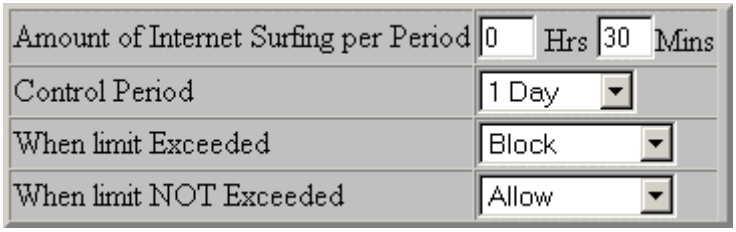
4. Check all the boxes between 9am and 11pm, and 2pm and 5pm, for the days Monday through to Friday

5. Click the *Save* button after making changes to apply the new configuration to ContentKeeper.

Configuring P.S.U Settings

To configure the *P.S.U* settings for any *Category*, select *PSU* from the drop-down in the *State* column of the *Categories* table, and then click on the associated *Settings* button. The *Personal Surfing Unit Settings* screen will be displayed.

Note: Refer to the Personal Surfing Units section in Chapter 4 for a complete explanation of the *PSU Blocking State*.



Configuring *P.S.Us* is a three-step process. The first step is to assign the desired amount of *P.S.Us*, the second step is to configure a *Control Period* and the third step is to configure *P.S.U Blocking States*. Once this process has been completed, the *P.S.U Global Parameters* should be reviewed, and reconfigured if necessary.

Assigning Personal Surfing Units

Use the *Amount of Internet Surfing per Period* input fields in the *Personal Surfing Unit Settings* table to assign the desired amount of *P.S.Us*. Assign *P.S.Us* by entering the desired value into the hours (Hrs) and/or minutes (Mins) input fields.

Configuring a Control Period

Configure the *P.S.U Control Period* by selecting the desired value, between one hour and one week, from the *Control Period* drop-down in the *Personal Surfing Unit Settings* table.

Configuring P.S.U Blocking States

The *P.S.U Blocking States* consist of two settings, a setting to tell ContentKeeper what to do when the specified *P.S.U* limit has been exceeded, and a setting to tell ContentKeeper what to do when the specified P.S.U limit has not been exceeded.

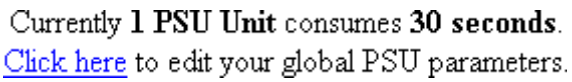
Select one of four *Blocking States* (*Allow*, *Block*, *Coach* or *Authenticate*) from the *When limit Exceeded* drop-down in the *Personal Surfing Unit Settings* table to tell ContentKeeper what to do when the specified *P.S.U* limit has been exceeded.

Select one of four *Blocking States* (*Allow*, *Block*, *Coach* or *Authenticate*) from the *When limit NOT Exceeded* drop-down in the *Personal Surfing Unit Settings* table to tell ContentKeeper what to do when the specified *P.S.U* limit has not been exceeded.

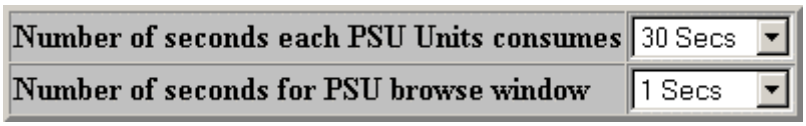
Click the *Save and Redisplay* button to apply your settings to ContentKeeper.

Configuring P.S.U Global Parameters

P.S.U Global Parameters may be accessed by clicking the *Click Here* hyperlink below the *Personal Surfing Unit Settings* table.



Note: Refer to the Personal Surfing Units section in Chapter 4 for an explanation of the *P.S.U Global Parameters*.



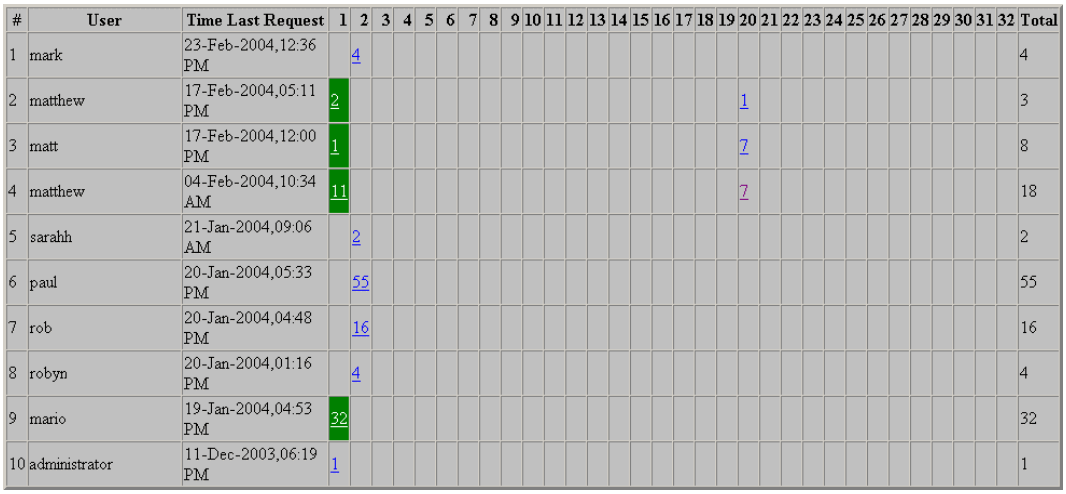
Configure the number of seconds that each *Personal Surfing Unit* consumes by selecting a value between one second and three hundred seconds from the *Number of seconds each P.S.U Unit consumes* drop-down in the *P.S.U Global Parameters* table.

Configure the size of the *PSU Browse Window* by selecting a value between one second and three hundred seconds from the *Number of seconds for PSU browse window* drop-down in the *P.S.U Global Parameters* table.

Click the *Save and Redisplay* button to apply your settings to ContentKeeper.

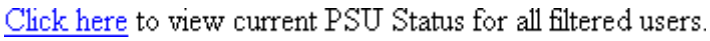
Viewing the P.S.U Control Status

The *P.S.U Control Status* table allows you to view the total number of *Personal Surfing Units* consumed by all users for all categories.



#	User	Time Last Request	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	Total
1	mark	23-Feb-2004,12:36 PM		4																															4
2	matthew	17-Feb-2004,05:11 PM	2																			1													3
3	matt	17-Feb-2004,12:00 PM	1																			7													8
4	matthew	04-Feb-2004,10:34 AM	11																			7													18
5	sarahh	21-Jan-2004,09:06 AM		2																															2
6	paul	20-Jan-2004,05:33 PM		55																															55
7	rob	20-Jan-2004,04:48 PM		16																															16
8	robyn	20-Jan-2004,01:16 PM		4																															4
9	mario	19-Jan-2004,04:53 PM	32																																32
10	administrator	11-Dec-2003,06:19 PM	1																																1

To view the *P.S.U Control Status* screen, click on the *Click Here* hyperlink at the bottom of the *P.S.U* settings screen, below the *P.S.U Global Parameters* hyperlink. The *P.S.U Control Status* screen will be opened in a separate browser window.



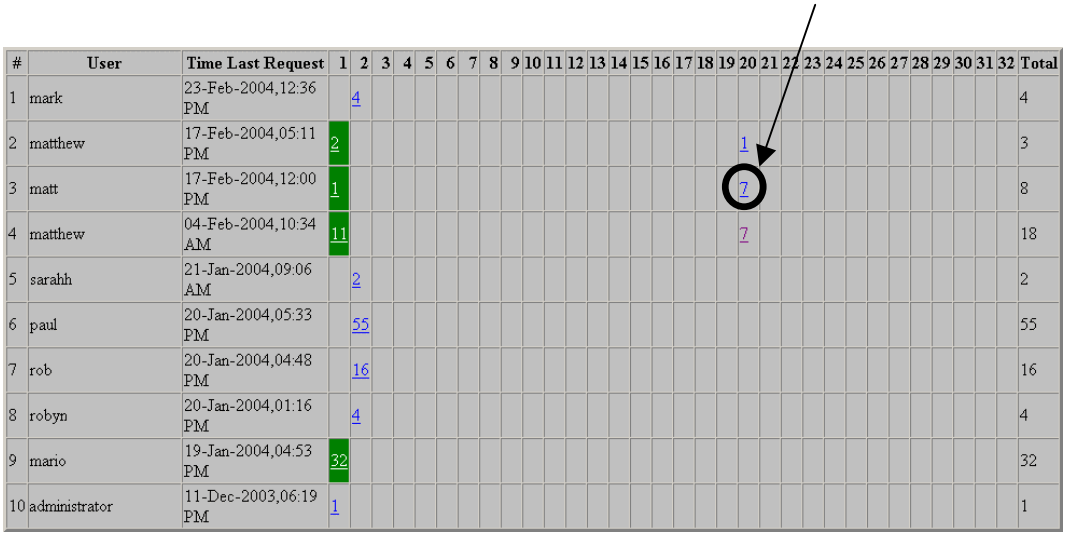
The *P.S.U Control Status* table consists of five columns, each of which is explained below:

- **# (Index)**- The *Index* column contains an index of each username entry for easy reference.
- **User** – The *User* column contains a list of all the users who have consumed one or more *P.S.Us*. Although a policy that has been configured with *P.S.Us* may apply to many users, a user will only appear in the *P.S.U Control Status* table after they have consumed one or more *P.S.Us.*
- **Time Last Request** – The *Time Last Request* column contains the time of the last URL request made by the associated user that consumed a *P.S.U*.
- **1-32 (Category) –** The *Category* column is actually thirty-two columns, each titled with a number from one to thirty-two, and representing one of the thirty-two *ContentKeeper Categories*. Each of the *Category* columns contains the number of *P.S.Us* consumed for that category by the associated user. Each number entry in the *Category* column is a hyperlink to the *P.S.U Usage Detail* tables for that category for the associated user. Refer to the Viewing P.S.U Usage Details section in this chapter for more information.

- **Total –** The *Total* column contains a figure representing the total number of *Personal Surfing Units* consumed by the associated user. This is a cross-category total, and therefore may contain a figure greater than the total number of allotted *P.S.Us* for any individual category.

Viewing P.S.U Usage Details

The *P.S.U Usage Details* screen may be accessed from the *P.S.U Control Status* screen by clicking on the desired hyperlink in the *Categories* column of the *P.S.U Control Status* table.



#	User	Time Last Request	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	Total
1	mark	23-Feb-2004,12:36 PM		4																															4
2	matthew	17-Feb-2004,05:11 PM	2																			1													3
3	matt	17-Feb-2004,12:00 PM	1																			7													8
4	matthew	04-Feb-2004,10:34 AM	11																			7													18
5	sarahh	21-Jan-2004,09:06 AM		2																															2
6	paul	20-Jan-2004,05:33 PM		55																															55
7	rob	20-Jan-2004,04:48 PM		16																															16
8	robyn	20-Jan-2004,01:16 PM		4																															4
9	mario	19-Jan-2004,04:53 PM	32																																32
10	administrator	11-Dec-2003,06:19 PM	1																																1

Note: Refer to the Viewing the P.S.U Control Status section in this chapter for more information on accessing the *P.S.U Control Status* screen.

The *P.S.U Usage Details* screen displays *P.S.U* statistics for the current user and the current category in the form of two tables.

(1)	Last Top Level URL/Domain Visited	www.google.com.au
(2)	Time of the last request	04-Feb-2004,10:33 a.m.
(3)	Number of PSU Units so far Consumed	7 Units
(4)	1 PSU Unit Currently Consumes	**15** Sec
(5)	Amount of Internet Surfing per Control Period	**30** Min
(6)	Length of Control Period	**1** Day
(7)	Start of Control Period	03-Feb-2004,4:53 p.m.
(8)	Amount of Control Period Used	**19** Day **21** Hr **57** Min **1** Sec

The first *P.S.U Usage Details Table contains* statistics about P.S.U settings and the cause of the most recently consumed P.S.Us. Each of the fields in *P.S.U Usage Details Table One* is defined below:

- **Row (1)** – *Row (1)* Contains the top level (parent) domain of the URL most recently visited by the selected user for the selected *Category* that consumed a *Personal Surfing Unit*. The URL appears as a hyperlink and will be opened in a new browser window if clicked.
- **Row (2)** – *Row (2)* contains the time of the most recent URL request by the selected user for the selected *Category* that consumed a *Personal Surfing Unit*.
- **Row (3)** – *Row (3)* contains the total number of a *Personal Surfing Units* consumed so far by the selected user for the selected *Category*.
- **Row (4)** – Row (4) contains the amount of time consumed by one *P.S.U.* This is a global parameter.
- **Row (5)** – Row (5) contains the amount of *P.S.U* time assigned to the selected user. This is a per Policy setting.
- **Row (6)** – Row (6) contains the amount of time in one *P.S.U Control Period*. This is a per Policy setting.
- **Row (7)** – Row (7) contains the time at the start of the *P.S.U Control Period*, which is when the selected user first consumed a *P.S.U* for the selected *Category*.
- **Row (8)** – Row (8) contains the amount of the *P.S.U Control Period* that has been used, or the amount of time that has passed since the *P.S.U Control Period* started.

(9)	Consumed PSU Time	**(3) * (4) = 1** Min **45** Sec
(10)	Surfing Time Remaining	**(5) - (9) = 28** Min **15** Sec
(11)	Current Status for this Category	**Allow**

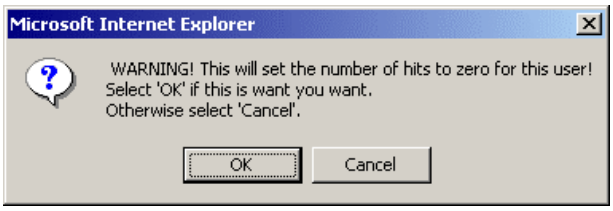
The second *P.S.U Usage Details Table contains* statistics about the total P.S.Us consumed. Each of the fields in *P.S.U Usage Details Table Two* is defined below:

- **Row (9)** – Row (9) contains the total *P.S.U* time consumed so far by the selected user for the selected *Category*. The value in this row is arrived at by multiplying the amount of time consumed by one *P.S.U* by the total number of a *Personal Surfing Units* consumed so far by the selected user for the selected *Category*.
- **Row (10)** – Row (10) contains the amount of *P.S.U* time remaining to the selected user for the selected *Category*. The value in this row is arrived at by subtracting the total *P.S.U* time consumed so far by the selected user for the selected *Category* from the amount of *P.S.U* time assigned to the selected user for the selected category.
- **Row (11)** – Row (11) contains the category state currently being applied by ContentKeeper to the selected user when they access URLs from the selected category.

Resetting Individual User P.S.U Controls

P.S.U Controls, the number of *P.S.Us* consumed, may be reset for an individual user by clicking the *Reset PSU* button at the bottom of the *P.S.U Usage Details* screen.

When the *Reset PSU* button is clicked you will be prompted to confirm the reset before it will take effect. Click *Yes* to confirm the action and reset the user *P.S.U Control* or click *Cancel* to abort.


Microsoft Internet Explorer
WARNING! This will set the number of hits to zero for this user!
Select 'OK' if this is want you want.
Otherwise select 'Cancel'.
OK
Cancel

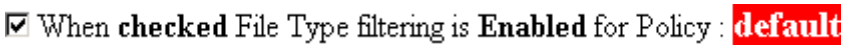
Note: Refer to the Viewing P.S.U Usage Details section in this chapter for more information on accessing the *P.S.U Usage Details* screen.

Configuring File-Types

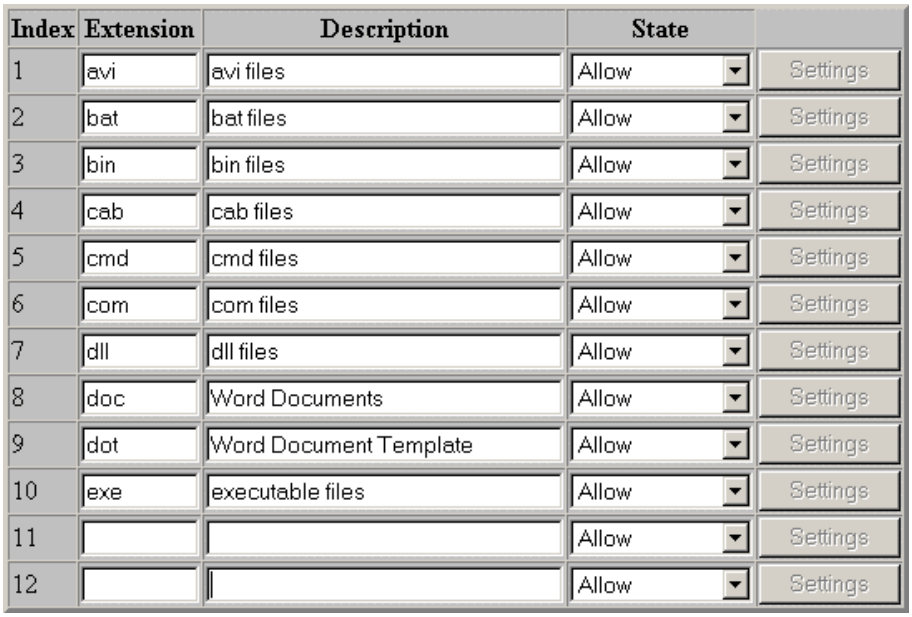
Main Menu – Blocking/Reporting → Create & Edit Policies → File-Types

ContentKeeper may be configured to filter files that are being downloaded via HTTP, i.e. files downloaded via an Internet browser. ContentKeeper may be configured to perform *File-Type* filtering for any policy from the *File-Types* menu. The *File-Types* menu may be accessed from the *Create & Edit Policies* menu by clicking on the *File-Types* button.

File-Type filtering is disabled by default and must be enabled before it may be configured. Click the check box at the bottom of the *File-Types* menu, labelled *When checked File Type filtering is Enabled for policy:* to enable or disable *File-Type* filtering.



Note: Settings in the *File-Types* menu are overridden by settings in the *Custom URLs* menu. Refer to the File-Types section in Chapter 4 for a complete explanation of ContentKeeper *File-Type* filtering.



Index	Extension	Description	State	
1	avi	avi files	Allow	Settings
2	bat	bat files	Allow	Settings
3	bin	bin files	Allow	Settings
4	cab	cab files	Allow	Settings
5	cmd	cmd files	Allow	Settings
6	com	com files	Allow	Settings
7	dll	dll files	Allow	Settings
8	doc	Word Documents	Allow	Settings
9	dot	Word Document Template	Allow	Settings
10	exe	executable files	Allow	Settings
11			Allow	Settings
12			Allow	Settings

The *File-Types* table consists of five columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each *File-Type* entry for easy reference.
- **Extension** – The *Extension* column accepts file extensions which may consist of letters and numbers, but must not include the dot '.' that usually separates the filename from the extension. Each entry in the extension column defines a different *File-Type* within ContentKeeper.
- **Description** – The *Description* column accepts a brief description of the *File-Type* in the associated *Extension* column.
- **State** – The *State* column contains a drop-down for each *File-Type* entry, which is used to configure the *Blocking State* for the associated *File-Type*. The *Blocking State* determines how ContentKeeper will filter files with the specified extension, for the current policy. Refer to the Blocking States section in Chapter 4 for an explanation of each *Blocking State* and how it affects *ContentKeeper File-Type Filtering*.
- **Settings** – The *Settings* column contains a *Settings* button for each *File-Type* entry. The *Settings* button only becomes available for the *T.O.D Blocking State*. Refer to the Time Of Day sections in this chapter for more information on configuring the *T.O.D Blocking State*.

To configure ContentKeeper to perform *File-Type* filtering, simply add the desired file type, defined by file extension, e.g. exe or bat, to the *File-Types* table and then assign it a *Blocking State*. Use the following procedure as a guide when configuring *File-Type* filtering:

1. Enter the desired file extension into the *Extension* input field of the *File-Types* table. Do not include a dot '.' when entering the file extension.

2. Enter a description of the desired file extension into the *Description* input field of the *File-Types* table.

3. Select a *Blocking State* from the *State* drop-down in the *File-Types* table.

4. Repeat the above steps as many times as necessary, then click *Save and Redisplay* to apply the new configuration to ContentKeeper.

Note: Refer to the Blocking States section in Chapter 4 for a complete explanation of *ContentKeeper Blocking States*.

Remember! Click the *Save and Redisplay* button after making changes to apply the new configuration to ContentKeeper.

Configuring Custom URLs

Main Menu – Blocking/Reporting → Create & Edit Policies → Custom URLs

Use the *Custom URLs* menu to define a list of individual URLs and associated *Blocking States*. *Custom URL Blocking States* will override *Category Blocking States* for the specified URLs. E.g. suppose that the *Sports* category is set to *Block* and the URL *www.sport.com* is in the *Custom URLs* list and set to Allow. If someone were to attempt to browse to *www.sport.com,* they would be allowed access, whereas all other sports sites would be blocked.

Entries in the *Custom URLs* menu will also override entries in the *File-Types* menu. E.g. suppose that *exe* extensions are set to *Block* in *File Types* and the file *update.exe* is set to allow in Custom URLs. If someone were to attempt to download *update.exe*, they would be allowed access to the file.

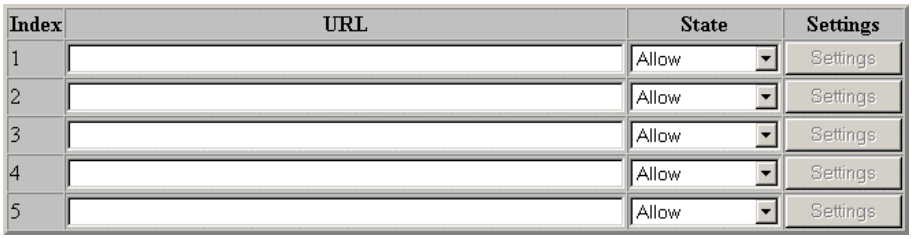
Important: In the *Custom URLs* menu, ContentKeeper treats .com as a URL component, not a file extension.

Mode of Operation

At the top of the *Custom URLs* menu there are four options, presented as radio buttons. These options govern how ContentKeeper processes URLs for the current policy. Any URL specified under this feature will be processed accordingly and not processed as part of the normal categories.

Important: The option specified here will effect how ContentKeeper processes all URLs for the current policy. Do not change from the *Default* option, until you understand the implications of doing so.

Note: Refer to the Custom URLs section under the Blocking Fundamentals section in Chapter 4 for a complete explanation of *ContentKeeper Custom URLs*, including an explanation of the *Mode of Operation* setting.



The *File-Types* table consists of five columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each *Custom URL* entry for easy reference.
- **URL** – The *URL* column accepts URLs, with or without URL arguments. URL and URL argument wild cards may be used in the *URL* column. Refer to the Custom URL Entry Rules section (below) in this chapter for a list of rules governing the entry of URLs.
- **State** – The *State* column contains a drop-down for each *Custom URL* entry, which is used to configure the *Blocking State* for the associated *Custom URL*. The *Blocking State* determines how ContentKeeper will filter files with the specified extension, for the current policy. Refer to the Blocking States section in Chapter 4 for an explanation of each *Blocking State* and how it affects *ContentKeeper Custom URL Filtering*.
- **Settings** – The *Settings* column contains a *Settings* button for each *Custom URL* entry. The *Settings* button only becomes available for the *T.O.D Blocking State*. Refer to the Time Of Day sections in this chapter for more information on configuring the *T.O.D Blocking State*.

Click the *Save and Redisplay* button after making changes to apply the new configuration to ContentKeeper.

Custom IP Addresses

IP addresses may be entered in to the Custom URLs menu by following the guidelines below:

- Only full 32-bit IP addresses may be entered into the Custom URLs menu, not parts of IP addresses, e.g. 192.9.200.67, not 192.9.200.*
- A default *Blocking State* for all target IP addresses may be configured by entering “xxx.xxx.xxx.xxx/” into the *Custom URLs* table. The result of this is that all IP addresses that are not explicitly mentioned further up the table from the entry, “xxx.xxx.xxx.xxx/”, will be processed by ContentKeeper according to the *State* setting for the “xxx.xxx.xxx.xxx/” entry.
- No wild cards may be used when entering IP addresses into the *Custom URLs* menu.
- Any entries into the *Custom URLs* table will only affect the current policy.

Custom URL Entry Rules

When making entries into the *Custom URLs* menu, please follow the rules below:

(General)

- Do not specify the protocol prefix, e.g. http://.
- Entries may be a maximum of 128 characters in length.
- Do not enter back slashes '\', only use forward slashes '/'.

(URL-Wildcard '*')

- There may be a maximum of 2 URL-wildcards per entry.
- *Custom URL* entries with 2 wildcards take priority over entries with only 1 wildcard, which take priority over entries with no wildcards.

  Click the *Save and Redisplay* button to automatically sort entries by priority.

- Wildcards must **not** be used when entering IP addresses.

(Argument-Wildcard '#')

- There may be a maximum of 2 argument-wildcards per entry.
- URLs and URL-arguments must be separated by a '?'.
- *Custom URL* entries with 2 argument-wildcards take priority over entries with only 1 argument-wildcard, which take priority over entries with no argument-wildcards. This rule applies to argument-wildcards independently of URL-wildcards.

  Click the *Save and Redisplay* button to automatically sort entries by priority.

- Argument-wildcards must **not** be used when entering IP addresses.

To view examples of *URL-wildcard* and *argument-wildcard* usage in *Custom URLs*, click the *Click Here for Examples* button at the bottom of the *Custom URLs* screen.

To configure ContentKeeper to perform *Custom URL* filtering, simply add the desired URL to the *Custom URLs* table and then assign it a *Blocking State*. Use the following procedure as a guide when configuring *Custom URL* filtering:

1. Enter the desired URL into the *URL* input field of the *Custom URLs* table.

2. Select a *Blocking State* from the *State* drop-down in the *Custom URLs* table.

3. Repeat the above steps as many times as necessary, then click *Save and Redisplay* to apply the new configuration to ContentKeeper.

Click the *Save and Redisplay* button after making changes to apply the new configuration to ContentKeeper.

Configuring Other Rules

Main Menu – Blocking/Reporting → Create & Edit Policies → Other Rules

Use the settings in the *Other Rules* menu to enable or disable blocking and reporting for the current policy. This is sometimes known as *Silent Mode*, and can be very useful for testing policies before they are enabled, without impacting on users.

Note: Refer to the Silent Mode section in Chapter 4 for more information on enabling and using *Silent Mode*.

Report Blocked URLs in Blocked Activity Report

Select *Yes* or *No* from the *Report Blocked URLs in Blocked Activity Report* drop-down to enable or disable the reporting of URLs blocked under the current policy.

When this option is set to *No*, ContentKeeper may continue to generate *blockpages* for URLs blocked under this policy, depending on what the *Generate a Blocking Page if URL Blocked* drop-down is set to, but will not report the blocking event in the *Current Blocking Activity* logs.

Generate a Blocking Page if URL Blocked

Select *Yes* or *No* from the *Generate a Blocking Page if URL Blocked* drop-down to enable or disable the generation of *blockpages* for URLs blocked under this policy.

When this option is set to *No*, ContentKeeper may continue to report URLs blocked under this policy, depending on what the *Report Blocked URLs in Blocked Activity Report* drop-down is set to, but will not generate *blockpages* for URLs blocked under this policy. Instead the requested URL will be allowed.

Click the *Save and Redisplay* button after making changes to apply the new configuration to ContentKeeper.

Display Policies

Main Menu – Blocking/Reporting → Display Policies

Use the *Display Policies* menu to gain an overview of all the policies that have been created, as well as see a detailed report of the *Default Policy*.

At the top of the *Display Policies* menu, two tables will be displayed. One is a *Current List of Policies*, and the other is a list of *Other Rules/Properties*. These tables allow an administrator to determine at a glance which policies are enabled, as well as which policies will generate a blocking page and which policies will only report a blocking page.

Current List of Policies

No.	Policy Name	Description	Enabled	Directory Service	Report	Verify
1	monitor-policy	monitor and report porn access	Yes	Local Database	Report	Verify
2	guest-policy	policy for temporary contractors	No	Local Database	Report	Verify
3	managers-policy	policy for managing directors	Yes	Local Database	Report	Verify
4	staff-policy	general staff policy	Yes	Local Database	Report	Verify
5	default	Default and catch all policy	Always	n/a	Report	Verify

Other Rules/Properties

No.	Policy Name	Block Report	Block Page
1	monitor-policy	Yes	No
2	guest-policy	Yes	Yes
3	managers-policy	Yes	Yes
4	staff-policy	Yes	Yes
5	default	Yes	Yes

These tables also allow an administrator to verify, and produce a report for each policy. Additionally, the tables contain hyperlinks to each policy for convenient access to the *Create & Edit Policies* menu.

Current List of Policies Table

The *Current List of Policies* table contains seven columns, each of which is defined below:

- **No. (Number)** – The *Number* column contains an index of each *Policy* for easy reference.
- **Policy Name** – The *Policy Name* column contains the name of the policies. Each policy name is a hyperlink to the *Create & Edit Policies* menu for that policy.
- **Description** – The *Description* column contains the description of each policy as it was entered when the policy was created.
- **Enabled** – The *Enabled* column indicates, by a value of *Yes* or *No*, whether a particular policy is currently enabled. Enabled policies have a value of *Yes*, which is highlighted.
- **Directory Service** – The *Directory Service* column contains the directory service that the policy is configured with.
- **Report** – The *Report* column contains a hyperlink, which causes the *Display Policies* menu to be redisplayed for the selected policy when clicked.
- **Verify** – The *Verify* column contains a hyperlink, which causes the *Verify Policy* menu to be displayed for the selected policy when clicked.

Other Rules/Properties Table

The *Other Rules/Properties* table contains four columns that represent the *Other Rules* settings for each policy; each of which is defined below:

- **No. (Number)** – The *Number* column contains an index of each *Policy* for easy reference.
- **Policy Name** – The *Policy Name* column contains the name of the policies. Each policy name is a hyperlink to the *Create & Edit Policies* menu for that policy.
- **Block Report** – The *Block Report* column indicates, by a value of *Yes* or *No*, whether the *Report Blocked URLs in Blocking/Click-Thru Activity Report* option in the *Other Rules* section of a particular policy is currently enabled. Enabled policies have a value of *Yes*.
- **Block Page** – The *Block Page* column indicates, by a value of *Yes* or *No*, whether the *Generate a Blocking Page if URL Blocked* option in the *Other Rules* section of a particular policy is currently enabled. Enabled policies have a value of *Yes*.

Verify Policy

Main Menu – Blocking/Reporting → Verify Policy

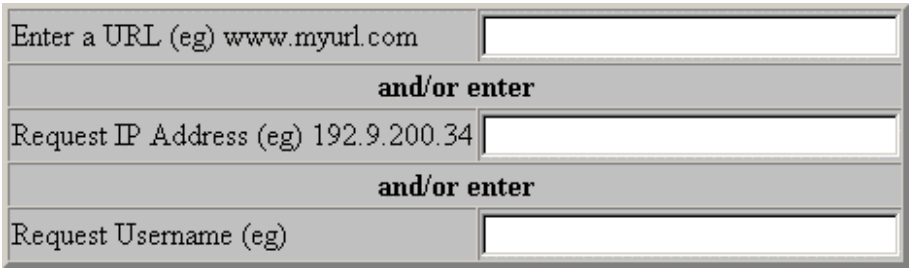
ContentKeeper incorporates a policy verification facility, which gives an administrator the ability to test policies in the following ways:

- Test the logic of the current individual policy.
- Test the logic of all policies including the current policy.

The policy verification tests may be performed offline, which means that they do not affect users by requiring a policy to be enabled. Once a policy has been verified and proven to produce the desired results, it may then be enabled with the confidence that it will perform as expected.

Note: Enable a policy by checking the enable check box in the *Create & Edit Policies* table, then clicking on the *Save and Redisplay* button. Refer to the Create & Edit Policies section in this chapter for more information on creating and enabling policies.

To verify an individual policy, select the desired policy from the *Select Policy* drop-down in the *Create & Edit Policies* table, and then click the *Verify* button in the same table. A *Policy Verifier Input* table will be displayed.



Enter a URL, appropriate to test the current policy, and then a username or an IP address into the appropriate input fields in the *Policy Verifier Input* table. Finally select a policy verification method by clicking on one of the buttons below the *Policy Verifier Input* table. Use the following sections as a guide to choosing the appropriate policy verification method.

Note: If you attempt to verify the policy against an IP address and there are no IP address *Directory Objects* associated with the policy, the default policy will be applied. The same principal applies to usernames.

Note: The *Category* under which a URL is categorised will affect the output of the Policy Verification facility. Refer to the Unique Categories section in Chapter 4 for more information.

Realtime Verification

Click on the *Realtime Verification* button to verify the URL and username/IP address combination against all currently enabled policies, ignoring currently disabled policies. When the *Realtime Verification* button is clicked, the *Policy Verifier Results* table will contain the phrase *Realtime Verification* in the *Policy to Verify* field of the *Input* section.

Verify Input on All Policies

Click on the *Verify Input on All Policies* button to verify the URL and username/IP address combination against all policies as though they were all currently enabled, regardless of whether any of them are currently disabled. When the *Verify Input on All Policies* button is clicked, the *Policy Verifier Results* table will contain the phrase *All Policies Enabled* in the *Policy to Verify* field of the *Input* section.

Verify Input on Policy

Click on the *Verify Input on Policy* button to verify the URL and username/IP address combination against the current policy only, as though it were enabled, and regardless of whether or not it is enabled. When the *Verify Input on Policy* button is clicked, the *Policy Verifier Results* table will contain the name of the current policy in the *Policy to Verify* field of the *Input* section.

Policy Verifier Results

After a method button has been clicked, the results of the policy verification are displayed in the *Policy Verifier Results* tables. There are two tables, the *Input* table and the *Output* table.

Input

Policy to verify	default
Request URL	www.playboy.com
Request IP Address	192.9.200.32
Request Username	jason

The *Input* table contains three fields that represent the entries made in the *Policy Verifier Input* table, each of which is explained below:

- **Policy to Verify** – The *Policy to Verify* field contains the policy, or policies against which the URL and username/IP address combination has been verified.
- **Request URL** – The *Request URL* field contains the URL specified in the *Policy Verifier Input* table.
- **Request IP Address** – The *Request IP Address* field contains the IP address specified in the *Policy Verifier Input* table. This field will not be present if no IP address was specified.
- **Request Username** – The *Request IP Username* field contains the username specified in the *Policy Verifier Input* table. This field will not be present if no username was specified.

Output

Status/Result	**Block**
Category	**Adult Content,Shopping,Entertainment (List Blocked)**
Policy	**Policy=default**
Report Blocked	**Yes**
Blocking Page	**Yes**
Policy State	**Currently Enabled**

The *Output* table contains three fields that represent the result of the policy verification procedure, each of which is defined below:

- **Status/Result** – The *Status/Result* field contains the actual result of processing the URL, i.e. what would happen if an actual user requested the URL (and the conditions being simulated by the Policy Verifier were true).
- **Category** – the *Category* field contains the category or categories, if any, under which the requested URL has been categorised.
- **Policy** – The *Policy* field contains the policy to which the simulated URL request was matched. This may or may not be the current policy, depending on the configuration of the current policy and which verification method was chosen.
- **Report Blocked** – The *Report Blocked* field contains a value of *Yes* or *No* and reflects the *Report Blocked URLs in Blocked Activity Report* setting in the *Other Rules* section of the policy that was matched to the URL request being verified.
- **Blocking Page** – The *Blocking Page* field contains a value of *Yes* or *No* and reflects the *Generate a Blocking Page if URL Blocked* setting in the *Other Rules* section of the policy that was matched to the URL request being verified.
- **Policy State** – The *Policy State* field contains the current state of the policy that was matched to the URL request being verified. This will be either *Currently Enabled* or *Currently Disabled*.

Category Aliases

Main Menu – Blocking/Reporting → Category Aliases

Select *Category Aliases* from the *Blocking/Reporting* menu to specify an alternate name, or alias, for any *Category*. Any aliases specified here would appear in the place of the standard category name in all *blockpages*; log files and reports.

This facility is particularly useful if the default category names do not suit your organisations policies, or if you wish category information to appear in another language.

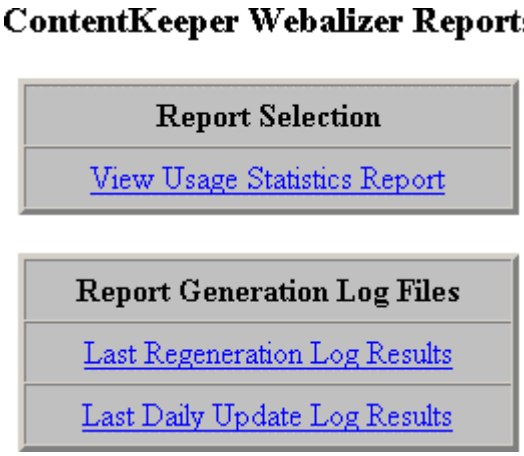
Index	Name	Alias	Index	Name	Alias
1	Pornography/Sex	Adult Content	17	www-Email Sites	www-Email Sites
2	News	News	18	Violence/Undesirable	Violence/Undesirable
3	Job Search	Job Search	19	Malicious	Malicious
4	Gambling	Gambling	20	Search Sites	Search Sites
5	Travel/Tourism	Travel/Tourism	21	Health Sites	Health Sites
6	Shopping	Shopping	22	Clubs and Societies	Clubs and Societies
7	Entertainment	Entertainment	23	Music Downloads	Music Downloads
8	Chatrooms	Chatrooms	24	Business Oriented	Business Oriented
9	Dating Sites	Dating Sites	25	Government Blocking List	Government Blocking List
10	Game Sites	Game Sites	26	Educational	Educational
11	Investment Sites	Investment Sites	27	Advertising	Advertising
12	E-Banking	E-Banking	28	Drugs/Alcohol	Drugs/Alcohol
13	Crime/Terrorism	Crime/Terrorism	29	Computing/IT	Computing/IT
14	Personal Beliefs/Cults	Personal Beliefs/Cults	30	Swimsuit/Lingerie/Models	Swimsuit/Lingerie/Models
15	Politics	Politics	31	null	Reserved
16	Sports	Sports	32	null	Reserved

To specify a *Category Alias*, click on the text box next to the chosen *Category* and replace the current name with a new one. Click the *Save* button after making changes to apply the new configuration to ContentKeeper.

Webalizer Reports

Main Menu – Blocking/Reporting → Webalizer Reports

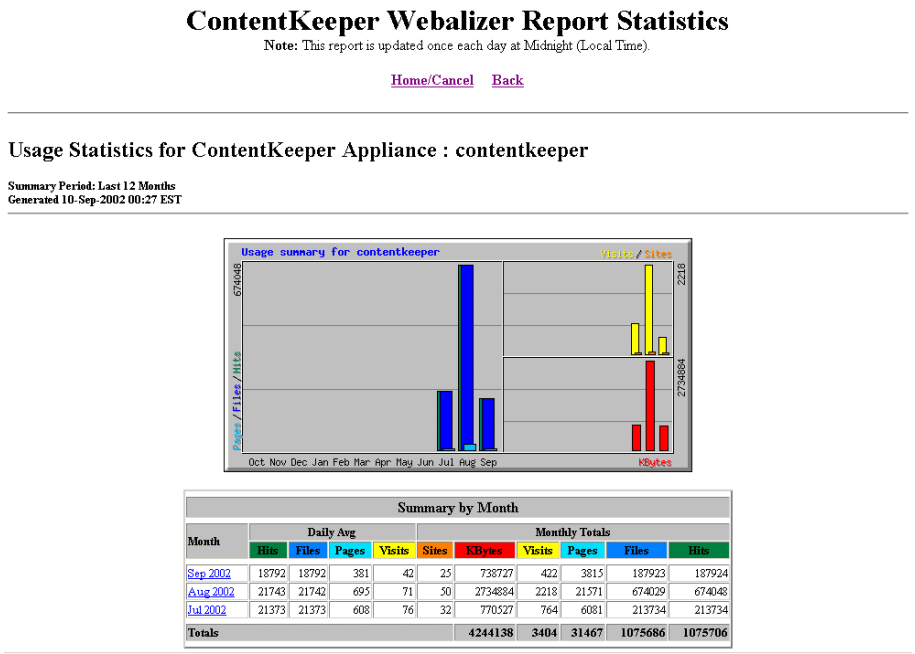
Select *Webalizer Reports* from the *Blocking/Reporting* menu to view reports on Internet activity. The reports displayed contain graphical and statistical data, including bar charts and tables of *Hits* on web sites, files downloaded, web pages downloaded, web pages requested, *Kilobytes* downloaded and most frequently visited URLs. Data is available for up to the last twelve months, and gives an overview of Internet activity for a selected time period. This information is useful in assessing how your Internet connection is being used and by which users.



Webalizer Report Statistics

The *Webalizer* statistics report contains a bar chart and a table. The bar chart represents a summary of the Internet usage over a twelve-month period for the network attached to ContentKeeper. The table contains statistics for the twelve-month period; detailing each month that *Webalizer* has data for. The table also contains a hyperlink for each month.

Click on the hyperlink for a month to display graphical and statistical data about that month.



ContentKeeper Webalizer Report Statistics

Note: This report is updated once each day at Midnight (Local Time).

Home/Cancel Back

Usage Statistics for ContentKeeper Appliance : contentkeeper

Summary Period: Last 12 Months
Generated 10-Sep-2002 00:27 EST

Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Sep 2002	18792	18792	381	42	25	738727	422	3815	187923	187924
Aug 2002	21743	21742	695	71	50	2734884	2218	21571	674029	674048
Jul 2002	21373	21373	608	76	32	770527	764	6081	213734	213734
Totals						**4244138**	**3404**	**31467**	**1075686**	**1075706**

Report Types and Totals

The yearly (index) report shows statistics for a 12-month period, and links to each month. The monthly report has detailed statistics for that month with additional links to any URL's and referrers found. To view a detailed report for any month, click on the name of that month. The various totals shown are explained below.

Monthly Statistics for September 2002		
Total Hits		187924
Total Files		187923
Total Pages		3815
Total Visits		422
Total KBytes		738727
Total Unique Sites		25
Total Unique URLs		32109
Total Unique Usernames		45
	Avg	Max
Hits per Hour	783	9967
Hits per Day	18792	62255
Files per Day	18792	62255
Pages per Day	381	957
Visits per Day	42	79
KBytes per Day	73873	143538
Hits by Response Code		
Undefined response code		1
Code 200 - OK		187923

Hits

Any request made to a web server which is logged, is considered a 'hit'. The requests can be for anything... html pages, graphic images, audio files, CGI scripts, etc... Each valid line in the server log is counted as a hit. This number represents the total number of requests that were made to web servers during the specified report period.

Files

Some requests made to a web server, require that the server then send something back to the requesting client, such as an html page or graphic image. When this happens, it is considered a 'file' and the files total is incremented. The relationship between 'hits' and 'files' can be thought of as 'incoming requests' and 'outgoing responses'.

Pages

Generally, any HTML document, or anything that generates an HTML document, would be considered a page. This does not include the other components that go into a document, such as graphic images, audio clips, etc... This number represents the number of 'pages' requested only, and does not include the other components that are in the page. What actually constitutes a 'page' can vary from server to server. Webalizer treats anything with the extension '.htm', '.html' or '.cgi' as a page.

Sites

Each request made to a server comes from a unique 'site', which can be referenced by a name or ultimately, an IP address. The 'sites' number shows how many unique IP addresses made requests to web servers during the reporting time period. This DOES NOT mean the number of unique individual users that visited. The Sites total is a general representation of the number of computers browsing the Internet from your network.

Note: It is possible that the Sites total will not accurately reflect the number of computers that are browsing the Internet from your network if, for example, the computers on your network connect to the Internet through a proxy server and the ContentKeeper server sits on the Internet side of that proxy server. In this situation, the number of sites would be reported as only one.

Visits

Whenever a request is made to a web server from a given IP address (site), the amount of time since a previous request by the address is calculated (if any). If the time difference is greater than a pre-configured 'visit timeout' value (or has never made a request before), it is considered a 'new visit', and this total is incremented (both for the site, and the IP address).

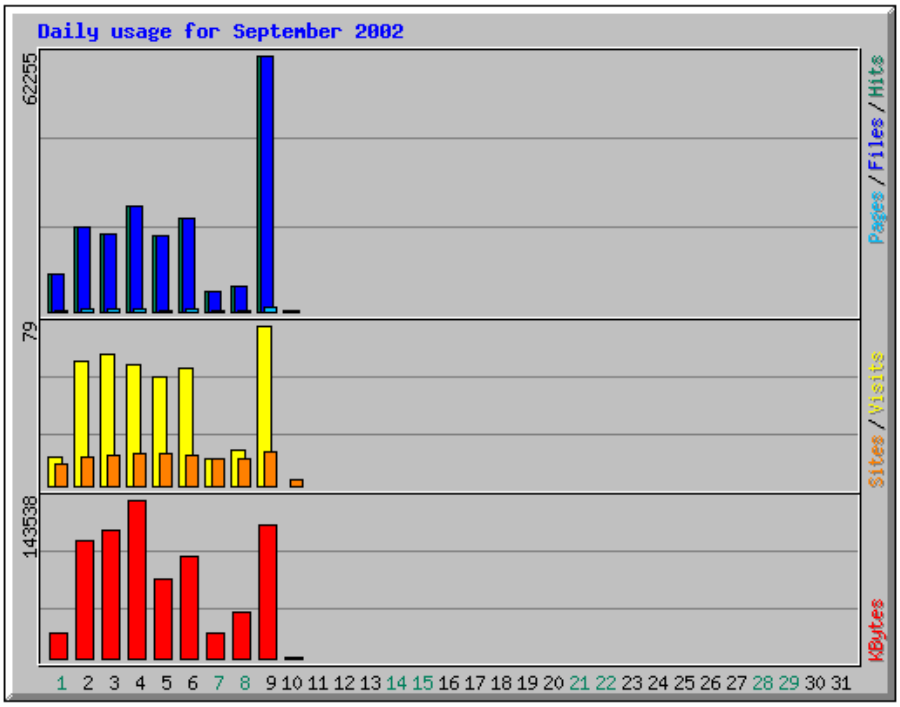
Note: in the 'Top Sites' table, the visits total should be discounted on 'Grouped' records, and thought of as the "Minimum number of visits" that came from that grouping instead.

Note: Visits only occur on PageType requests, that is, for any request whose URL is one of the 'page' types (i.e. htm, html, cgi). Due to the limitation of the HTTP protocol, log rotations and other factors, this number should not be taken as absolute, rather, it should be considered to be an estimate only.

Kbytes

The KBytes (kilobytes) value shows the amount of data, in KB, that was sent out by all web servers during the specified reporting period.

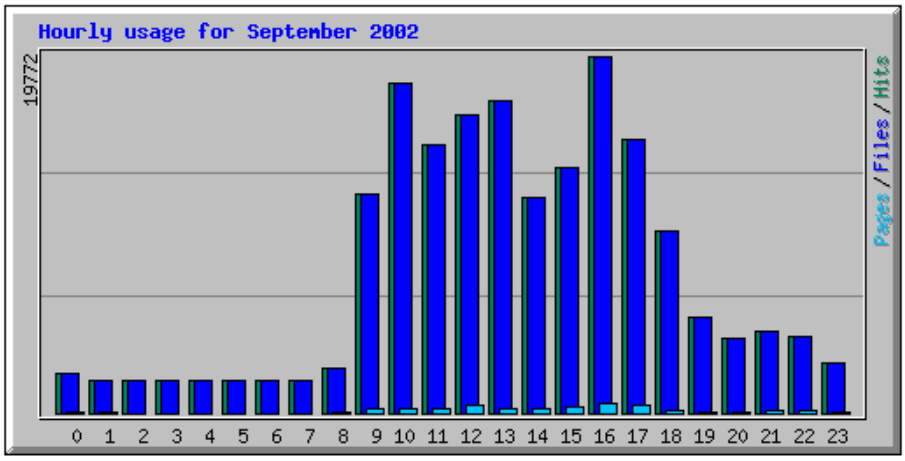
Note: A kilobyte is 1024 bytes, not 1000 bytes.



Daily Statistics for September 2002

Day	Hits		Files		Pages		Visits		Sites		KBytes	
1	9068	4.83%	9068	4.83%	49	1.28%	14	3.32%	11	44.00%	22717	3.08%
2	20384	10.85%	20384	10.85%	543	14.23%	61	14.45%	14	56.00%	107017	14.49%
3	18904	10.06%	18904	10.06%	472	12.37%	65	15.40%	15	60.00%	116466	15.77%
4	25448	13.54%	25447	13.54%	716	18.77%	60	14.22%	16	64.00%	143538	19.43%
5	18527	9.86%	18527	9.86%	401	10.51%	54	12.80%	16	64.00%	71036	9.62%
6	22526	11.99%	22526	11.99%	515	13.50%	58	13.74%	15	60.00%	92909	12.58%
7	4717	2.51%	4717	2.51%	41	1.07%	13	3.08%	13	52.00%	22870	3.10%
8	6077	3.23%	6077	3.23%	121	3.17%	18	4.27%	13	52.00%	41427	5.61%
9	62255	33.13%	62255	33.13%	957	25.09%	79	18.72%	17	68.00%	120613	16.33%
10	18	0.01%	18	0.01%	0	0.00%	0	0.00%	3	12.00%	134	0.02%

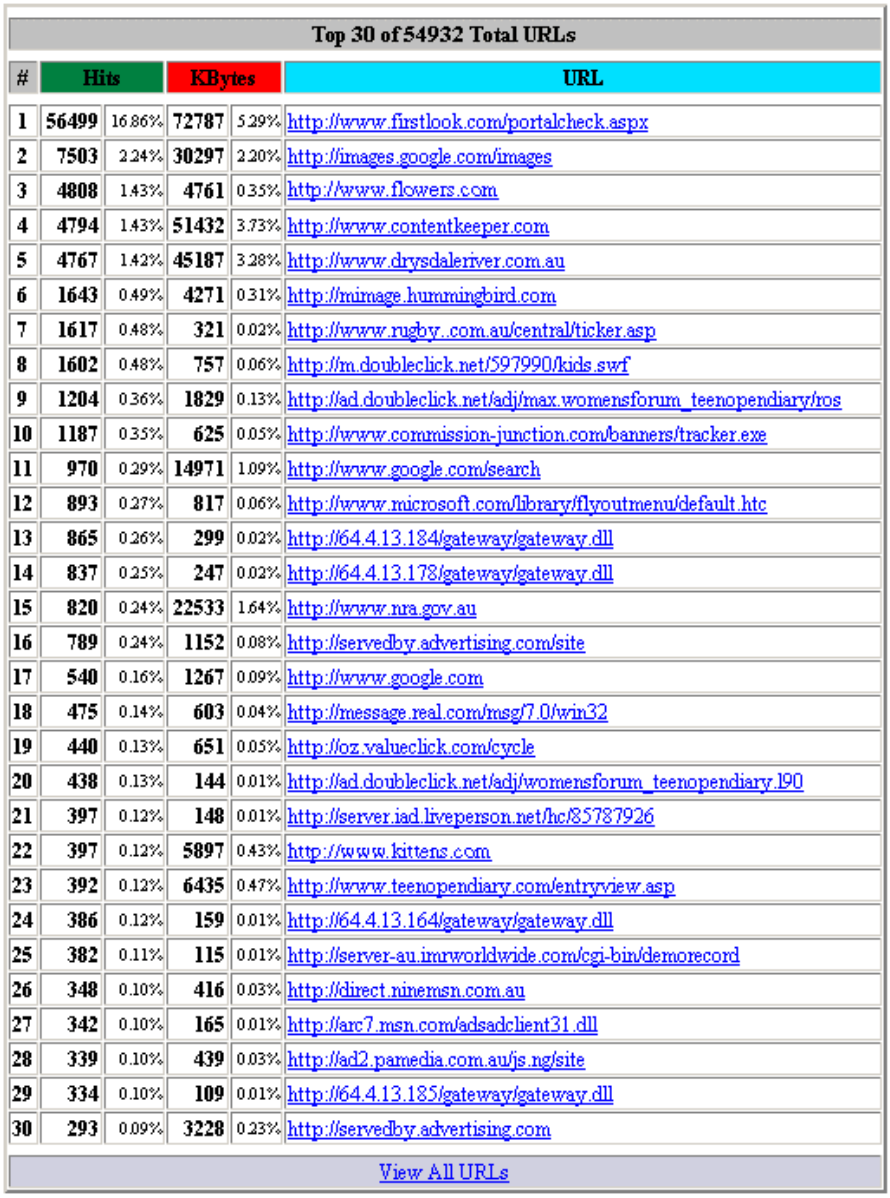
The Monthly, Daily and Hourly Usage Statistics reports are a collection of Bar charts and tables that display information about Hits, Files, Pages and Sites which detail the number of requests made to web servers for each visit to each site by every user as well as information about files downloaded from each web server.



Hourly Statistics for September 2002

Hour	Hits			Files			Pages			KBytes		
	Avg	Total		Avg	Total		Avg	Total		Avg	Total	
0	216	2161	1.15%	216	2161	1.15%	0	9	0.24%	786	7862	1.06%
1	184	1845	0.98%	184	1845	0.98%	0	3	0.08%	522	5216	0.71%
2	180	1808	0.96%	180	1808	0.96%	0	0	0.00%	473	4732	0.64%
3	181	1811	0.96%	181	1811	0.96%	0	0	0.00%	455	4549	0.62%
4	179	1795	0.96%	179	1795	0.96%	0	0	0.00%	458	4578	0.62%
5	180	1803	0.96%	180	1803	0.96%	0	0	0.00%	453	4526	0.61%
6	180	1802	0.96%	180	1802	0.96%	0	0	0.00%	453	4533	0.61%
7	177	1775	0.94%	177	1775	0.94%	0	0	0.00%	728	7285	0.99%
8	252	2523	1.34%	252	2523	1.34%	5	59	1.55%	1557	15568	2.11%
9	1213	12133	6.46%	1213	12133	6.46%	24	248	6.50%	6407	64066	8.67%
10	1829	18299	9.74%	1829	18299	9.74%	28	288	7.55%	7678	76776	10.39%
11	1489	14899	7.93%	1489	14899	7.93%	28	287	7.52%	4439	44388	6.01%
12	1649	16493	8.78%	1649	16493	8.78%	40	404	10.59%	5111	51112	6.92%
13	1728	17281	9.20%	1728	17281	9.20%	25	252	6.61%	3192	31923	4.32%
14	1190	11903	6.33%	1190	11903	6.33%	25	250	6.55%	4501	45013	6.09%
15	1356	13562	7.22%	1356	13562	7.22%	36	363	9.52%	8271	82710	11.20%
16	1977	19772	10.52%	1977	19772	10.52%	51	511	13.39%	9349	93492	12.66%
17	1511	15112	8.04%	1511	15111	8.04%	43	432	11.32%	4988	49883	6.75%
18	1012	10129	5.39%	1012	10129	5.39%	19	193	5.06%	3694	36943	5.00%
19	530	5309	2.83%	530	5309	2.83%	8	82	2.15%	2595	25952	3.51%
20	417	4171	2.22%	417	4171	2.22%	9	94	2.46%	1212	12121	1.64%
21	450	4504	2.40%	450	4504	2.40%	16	163	4.27%	2665	26646	3.61%
22	424	4243	2.26%	424	4243	2.26%	12	127	3.33%	2340	23397	3.17%
23	279	2791	1.49%	279	2791	1.49%	5	50	1.31%	1546	15457	2.09%

The data shown within the *Hourly Usage Statistics* chart and table is an average of the hourly statistics for each day of the month. An average daily usage pattern may be obtained by viewing the *Hourly Usage Statistics* bar chart.



Top 30 of 54932 Total URLs

#	Hits		KBytes		URL
1	56499	16.86%	72787	5.29%	http://www.firstlook.com/portalcheck.aspx
2	7503	2.24%	30297	2.20%	http://images.google.com/images
3	4808	1.43%	4761	0.35%	http://www.flowers.com
4	4794	1.43%	51432	3.73%	http://www.contentkeeper.com
5	4767	1.42%	45187	3.28%	http://www.drysdaleriver.com.au
6	1643	0.49%	4271	0.31%	http://mimage.hummingbird.com
7	1617	0.48%	321	0.02%	http://www.rugby..com.au/central/ticker.asp
8	1602	0.48%	757	0.06%	http://m.doubleclick.net/597990/kids.swf
9	1204	0.36%	1829	0.13%	http://ad.doubleclick.net/adj/max.womensforum_teenopendiary/ros
10	1187	0.35%	625	0.05%	http://www.commission-junction.com/banners/tracker.exe
11	970	0.29%	14971	1.09%	http://www.google.com/search
12	893	0.27%	817	0.06%	http://www.microsoft.com/library/flyoutmenu/default.htc
13	865	0.26%	299	0.02%	http://64.4.13.184/gateway/gateway.dll
14	837	0.25%	247	0.02%	http://64.4.13.178/gateway/gateway.dll
15	820	0.24%	22533	1.64%	http://www.nra.gov.au
16	789	0.24%	1152	0.08%	http://servedby.advertising.com/site
17	540	0.16%	1267	0.09%	http://www.google.com
18	475	0.14%	603	0.04%	http://message.real.com/msg/7.0/win32
19	440	0.13%	651	0.05%	http://oz.valueclick.com/cycle
20	438	0.13%	144	0.01%	http://ad.doubleclick.net/adj/womensforum_teenopendiary.l90
21	397	0.12%	148	0.01%	http://server.iad.liveperson.net/hc/85787926
22	397	0.12%	5897	0.43%	http://www.kittens.com
23	392	0.12%	6435	0.47%	http://www.teenopendiary.com/entryview.asp
24	386	0.12%	159	0.01%	http://64.4.13.164/gateway/gateway.dll
25	382	0.11%	115	0.01%	http://server-au.imrworldwide.com/cgi-bin/demorecord
26	348	0.10%	416	0.03%	http://direct.ninemsn.com.au
27	342	0.10%	165	0.01%	http://arc7.msn.com/adsadclient31.dll
28	339	0.10%	439	0.03%	http://ad2.pamedia.com.au/js.ng/site
29	334	0.10%	109	0.01%	http://64.4.13.185/gateway/gateway.dll
30	293	0.09%	3228	0.23%	http://servedby.advertising.com

View All URLs

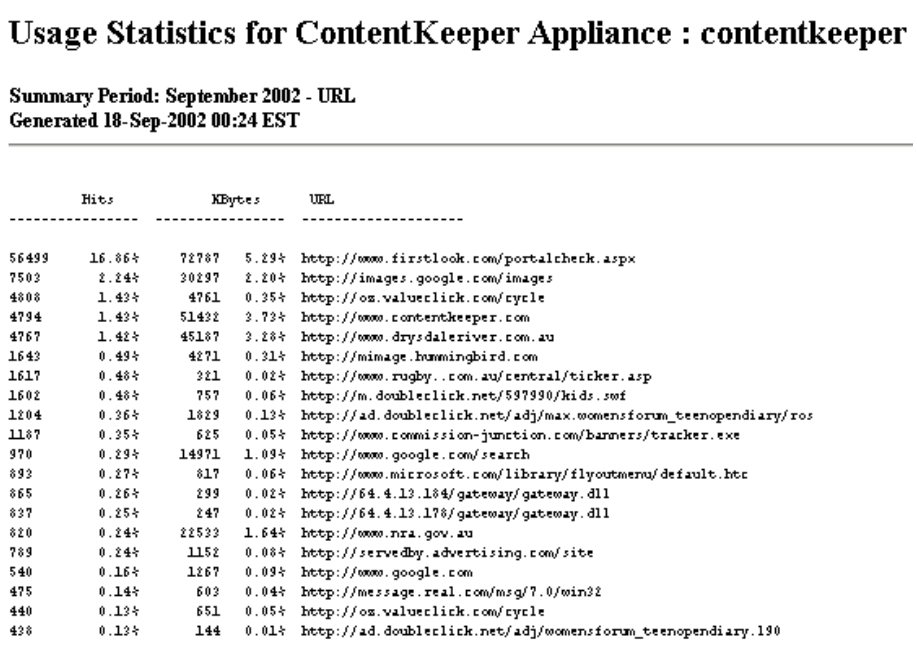
Many of the tables and charts in the *Webalizer Report* contain only the top, or first, few items. The complete lists may be viewed by clicking the *View All* hyperlink at the bottom of the chart or table, where available.

Top 30 of 54932 Total URLs By KBytes					
#	Hits		KBytes		URL
1	56499	16.86%	72787	5.29%	http://www.firstlook.com/portalcheck.aspx
2	3	0.00%	51780	3.76%	http://nds1.forum.nokia.com/nds/nds_tverification_interface
3	4794	1.43%	51432	3.73%	http://www.contentkeeper.com
4	4767	1.42%	45187	3.28%	http://www.drysdaleriver.com.au
5	77	0.02%	39988	2.90%	http://www.logitech.com.au
6	7503	2.24%	30297	2.20%	http://images.google.com/images
7	1	0.00%	24458	1.78%	http://ftp.hp.com/pub/ccd/keeper2sdd/mobile/agfxk00.exe
8	820	0.24%	22533	1.64%	http://www.nra.gov.au
9	61	0.02%	20843	1.51%	http://www.download.windowsupdate.com
10	43	0.01%	19096	1.39%	http://www.secondlook.com/index.cfml
11	3	0.00%	18796	1.36%	http://a256.g.akamai.net
12	10	0.00%	17505	1.27%	http://download.microsoft.com
13	970	0.29%	14971	1.09%	http://www.google.com/search
14	35	0.01%	14450	1.05%	http://crl.verisign.com/class3internationalserver.crl
15	278	0.08%	14358	1.04%	http://www.meow.net/switch/myex.iso
16	10	0.00%	13226	0.96%	http://www.contentkeeper.com/pdfs/contentkeeper20administration20guide20114a.pdf
17	1	0.00%	12108	0.88%	http://aoaftp3.aopen.com/pub/driver/vga/unidriver/winme9x_2942.exe
18	12	0.00%	8356	0.61%	http://crl.verisign.com/rsasecureserver.crl
19	1	0.00%	8124	0.59%	http://203.220.0.50/06b09c7933939d4b1f05/windows/realoneplayerv2beta.exe
20	6	0.00%	7274	0.53%	http://ftp6.ipswitch.com/ipswitch/product_downloads/f_x86t32.exe
21	190	0.06%	7236	0.53%	http://www.mittens.org
22	3	0.00%	7210	0.52%	http://www.math.u-bordeaux.fr/~depouill/xe3/xe3.iso
23	3	0.00%	6535	0.47%	http://www.powersauce.net/wegotthepower.asp
24	392	0.12%	6435	0.47%	http://www.teenopendiary.com/entryview.asp
25	1	0.00%	6210	0.45%	http://www.small.com/default.asp
26	293	0.09%	6034	0.44%	http://www.teenopendiary.com/entrylist.asp
27	397	0.12%	5897	0.43%	http://www.meltdown.com/hsgdt127hd/image.jpg
28	2	0.00%	5844	0.42%	http://www.math.u-bordeaux.fr/~depouill/xe3/kernel-2.2.16-3.i686.rpm
29	27	0.01%	5682	0.41%	http://netshow.ninemsn.com.au/living/ralph/emma_wilson_hi.wmv
30	20	0.01%	5189	0.38%	http://www.apache.org/dist/httpd/binaries/win32/apache_1.3.26-win32-x86-no_src.msi

Top 25 of 25 Total Sites									
#	Hits		Files		KBytes		Visits		Hostname
1	70493	37.51%	70492	37.51%	338448	45.81%	193	45.73%	192.9.200.4
2	39284	20.90%	39284	20.90%	66522	9.00%	48	11.37%	192.9.200.32
3	33859	18.02%	33859	18.02%	78787	10.67%	56	13.27%	192.9.200.194
4	15495	8.25%	15495	8.25%	43394	5.87%	22	5.21%	192.9.200.195
5	8098	4.31%	8098	4.31%	65020	8.80%	0	0.00%	192.9.200.10
6	7579	4.03%	7579	4.03%	12348	1.67%	14	3.32%	192.9.200.252
7	3443	1.83%	3443	1.83%	29405	3.98%	27	6.40%	192.9.200.246
8	1844	0.98%	1844	0.98%	13775	1.86%	10	2.37%	192.9.200.9
9	1836	0.98%	1836	0.98%	18791	2.54%	21	4.98%	192.9.200.33
10	1632	0.87%	1632	0.87%	3104	0.42%	4	0.95%	192.9.200.228
11	1243	0.66%	1243	0.66%	23464	3.18%	6	1.42%	192.9.200.18
12	1043	0.56%	1043	0.56%	10382	1.41%	9	2.13%	192.9.200.196
13	542	0.29%	542	0.29%	1898	0.26%	3	0.71%	192.9.200.226
14	416	0.22%	416	0.22%	2594	0.35%	1	0.24%	192.9.200.218
15	286	0.15%	286	0.15%	2458	0.33%	1	0.24%	192.9.200.243
16	277	0.15%	277	0.15%	3531	0.48%	0	0.00%	192.9.200.5
17	233	0.12%	233	0.12%	784	0.11%	2	0.47%	192.9.200.227
18	197	0.10%	197	0.10%	20243	2.74%	1	0.24%	192.9.200.31
19	46	0.02%	46	0.02%	3057	0.41%	0	0.00%	192.9.200.34
20	29	0.02%	29	0.02%	439	0.06%	2	0.47%	192.9.200.216
21	21	0.01%	21	0.01%	20	0.00%	2	0.47%	192.9.200.245
22	14	0.01%	14	0.01%	239	0.03%	0	0.00%	192.9.200.35
23	9	0.00%	9	0.00%	12	0.00%	0	0.00%	192.9.200.17
24	3	0.00%	3	0.00%	4	0.00%	0	0.00%	192.9.200.70
25	2	0.00%	2	0.00%	11	0.00%	0	0.00%	192.9.200.42

Top 25 of 25 Total Sites By KBytes									
#	Hits		Files		KBytes		Visits		Hostname
1	70493	37.51%	70492	37.51%	338448	45.81%	193	45.73%	192.9.200.4
2	33859	18.02%	33859	18.02%	78787	10.67%	56	13.27%	192.9.200.194
3	39284	20.90%	39284	20.90%	66522	9.00%	48	11.37%	192.9.200.32
4	8098	4.31%	8098	4.31%	65020	8.80%	0	0.00%	192.9.200.10
5	15495	8.25%	15495	8.25%	43394	5.87%	22	5.21%	192.9.200.195
6	3443	1.83%	3443	1.83%	29405	3.98%	27	6.40%	192.9.200.246
7	1243	0.66%	1243	0.66%	23464	3.18%	6	1.42%	192.9.200.18
8	197	0.10%	197	0.10%	20243	2.74%	1	0.24%	192.9.200.31
9	1836	0.98%	1836	0.98%	18791	2.54%	21	4.98%	192.9.200.33
10	1844	0.98%	1844	0.98%	13775	1.86%	10	2.37%	192.9.200.9
11	7579	4.03%	7579	4.03%	12348	1.67%	14	3.32%	192.9.200.252
12	1043	0.56%	1043	0.56%	10382	1.41%	9	2.13%	192.9.200.196
13	277	0.15%	277	0.15%	3531	0.48%	0	0.00%	192.9.200.5
14	1632	0.87%	1632	0.87%	3104	0.42%	4	0.95%	192.9.200.228
15	46	0.02%	46	0.02%	3057	0.41%	0	0.00%	192.9.200.34
16	416	0.22%	416	0.22%	2594	0.35%	1	0.24%	192.9.200.218
17	286	0.15%	286	0.15%	2458	0.33%	1	0.24%	192.9.200.243
18	542	0.29%	542	0.29%	1898	0.26%	3	0.71%	192.9.200.226
19	233	0.12%	233	0.12%	784	0.11%	2	0.47%	192.9.200.227
20	29	0.02%	29	0.02%	439	0.06%	2	0.47%	192.9.200.216
21	14	0.01%	14	0.01%	239	0.03%	0	0.00%	192.9.200.35
22	21	0.01%	21	0.01%	20	0.00%	2	0.47%	192.9.200.245
23	9	0.00%	9	0.00%	12	0.00%	0	0.00%	192.9.200.17
24	2	0.00%	2	0.00%	11	0.00%	0	0.00%	192.9.200.42
25	3	0.00%	3	0.00%	4	0.00%	0	0.00%	192.9.200.70

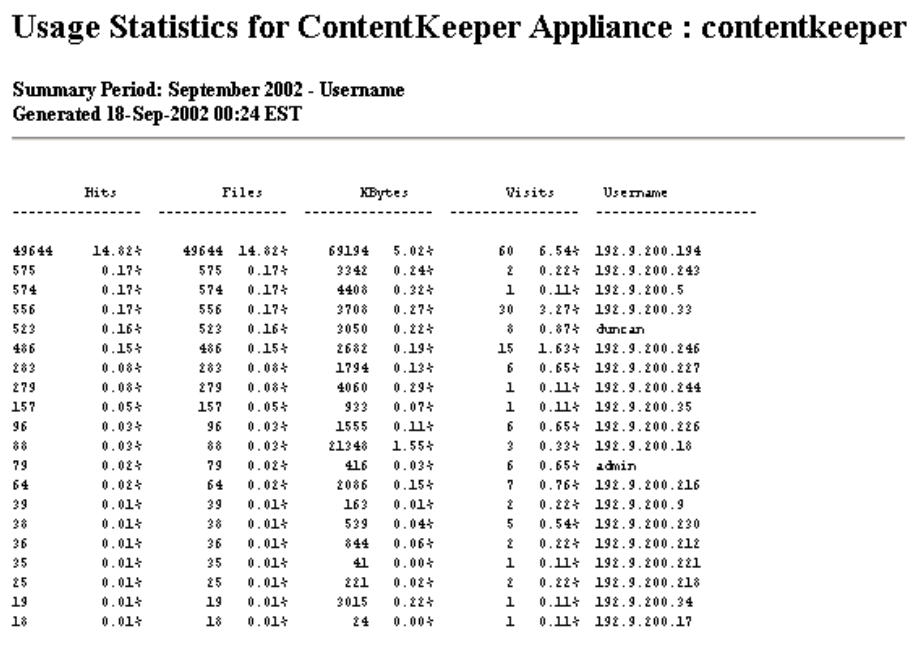
Top 30 of 54 Total Usernames									
#	Hits		Files		KBytes		Visits		Username
1	49644	14.82%	49644	14.82%	69194	5.02%	60	6.54%	192.9.200.194
2	46142	13.77%	46142	13.77%	128008	9.30%	78	8.50%	veronica
3	43008	12.84%	43008	12.84%	239696	17.41%	174	18.95%	allan
4	30702	9.16%	30702	9.16%	96669	7.02%	151	16.45%	tim
5	22132	6.61%	22132	6.61%	56663	4.11%	92	10.02%	peter
6	21662	6.47%	21662	6.47%	66251	4.81%	116	12.64%	christine
7	15160	4.52%	15160	4.52%	122425	8.89%	1	0.11%	192.9.200.10
8	14201	4.24%	14201	4.24%	45977	3.34%	86	9.37%	roger
9	14125	4.22%	14125	4.22%	43568	3.16%	39	4.25%	192.9.200.195
10	10890	3.25%	10890	3.25%	51971	3.77%	53	5.77%	paul
11	10871	3.24%	10871	3.24%	146794	10.66%	192	20.92%	192.9.200.4
12	10685	3.19%	10685	3.19%	51646	3.75%	50	5.45%	david
13	9902	2.96%	9902	2.96%	26510	1.93%	47	5.12%	danni
14	6389	1.91%	6389	1.91%	8735	0.63%	8	0.87%	192.9.200.252
15	5074	1.51%	5074	1.51%	34405	2.50%	37	4.03%	aaron
16	4921	1.47%	4921	1.47%	18160	1.32%	36	3.92%	brett
17	4439	1.32%	4439	1.32%	37793	2.74%	28	3.05%	steven
18	2957	0.88%	2957	0.88%	14141	1.03%	28	3.05%	john
19	2189	0.65%	2189	0.65%	12611	0.92%	21	2.29%	hannah
20	1892	0.56%	1892	0.56%	16346	1.19%	14	1.53%	192.9.200.196
21	1369	0.41%	1369	0.41%	1028	0.07%	7	0.76%	192.9.200.228
22	1171	0.35%	1171	0.35%	24784	1.80%	49	5.34%	192.9.200.32
23	891	0.27%	891	0.27%	4900	0.36%	3	0.33%	192.9.200.245
24	629	0.19%	629	0.19%	4482	0.33%	3	0.33%	tim
25	575	0.17%	575	0.17%	3342	0.24%	2	0.22%	192.9.200.243
26	574	0.17%	574	0.17%	4408	0.32%	1	0.11%	192.9.200.5
27	556	0.17%	556	0.17%	3708	0.27%	30	3.27%	192.9.200.33
28	523	0.16%	523	0.16%	3050	0.22%	8	0.87%	duncan
29	486	0.15%	486	0.15%	2682	0.19%	15	1.63%	192.9.200.246
30	283	0.08%	283	0.08%	1794	0.13%	6	0.65%	192.9.200.227
View All Usernames									



Usage Statistics for ContentKeeper Appliance : contentkeeper

Summary Period: September 2002 - URL
Generated 18-Sep-2002 00:24 EST

Hits		KBytes		URL
56499	16.86%	72787	5.29%	http://www.firstlook.com/portalcheck.aspx
7503	2.24%	30297	2.20%	http://images.google.com/images
4808	1.43%	4761	0.35%	http://ox.valueclick.com/cycle
4794	1.43%	51432	3.73%	http://www.contentkeeper.com
4767	1.42%	45187	3.28%	http://www.drysdaleriver.com.au
1643	0.49%	4271	0.31%	http://mimage.hummingbird.com
1617	0.48%	321	0.02%	http://www.rugby..com.au/central/ticker.asp
1602	0.48%	757	0.06%	http://m.doubleclick.net/597990/kids.swf
1204	0.36%	1829	0.13%	http://ad.doubleclick.net/adj/max.womensforum_teenopendiary/ros
1187	0.35%	625	0.05%	http://www.commission-junction.com/banners/tracker.exe
970	0.29%	14971	1.09%	http://www.google.com/search
893	0.27%	817	0.06%	http://www.microsoft.com/library/flyoutmenu/default.htc
865	0.26%	299	0.02%	http://64.4.13.184/gateway/gateway.dll
837	0.25%	247	0.02%	http://64.4.13.178/gateway/gateway.dll
820	0.24%	22533	1.64%	http://www.nra.gov.au
789	0.24%	1152	0.08%	http://servedby.advertising.com/site
540	0.16%	1267	0.09%	http://www.google.com
475	0.14%	603	0.04%	http://message.real.com/msg/7.0/win32
440	0.13%	651	0.05%	http://ox.valueclick.com/cycle
438	0.13%	144	0.01%	http://ad.doubleclick.net/adj/womensforum_teenopendiary.190



Usage Statistics for ContentKeeper Appliance : contentkeeper

Summary Period: September 2002 - Username
Generated 18-Sep-2002 00:24 EST

Hits		Files		KBytes		Visits		Username
49644	14.82%	49644	14.82%	69194	5.02%	60	6.54%	192.9.200.194
575	0.17%	575	0.17%	3342	0.24%	2	0.22%	192.9.200.243
574	0.17%	574	0.17%	4408	0.32%	1	0.11%	192.9.200.5
556	0.17%	556	0.17%	3708	0.27%	30	3.27%	192.9.200.33
523	0.16%	523	0.16%	3050	0.22%	8	0.87%	duncan
486	0.15%	486	0.15%	2682	0.19%	15	1.63%	192.9.200.246
283	0.08%	283	0.08%	1794	0.13%	6	0.65%	192.9.200.227
279	0.08%	279	0.08%	4060	0.29%	1	0.11%	192.9.200.244
157	0.05%	157	0.05%	933	0.07%	1	0.11%	192.9.200.35
96	0.03%	96	0.03%	1555	0.11%	6	0.65%	192.9.200.226
88	0.03%	88	0.03%	21348	1.55%	3	0.33%	192.9.200.18
79	0.02%	79	0.02%	416	0.03%	6	0.65%	admin
64	0.02%	64	0.02%	2086	0.15%	7	0.76%	192.9.200.216
39	0.01%	39	0.01%	163	0.01%	2	0.22%	192.9.200.9
38	0.01%	38	0.01%	529	0.04%	5	0.54%	192.9.200.230
36	0.01%	36	0.01%	844	0.06%	2	0.22%	192.9.200.212
35	0.01%	35	0.01%	41	0.00%	1	0.11%	192.9.200.221
25	0.01%	25	0.01%	221	0.02%	2	0.22%	192.9.200.218
19	0.01%	19	0.01%	3015	0.22%	1	0.11%	192.9.200.34
18	0.01%	18	0.01%	24	0.00%	1	0.11%	192.9.200.17

Advanced Reporting Module

Main Menu – Blocking/Reporting → Advanced Reporting Module

Clicking on the *Advanced Reporting Module* hyperlink will open the *Advanced Reporting Module* download page of the ContentKeeper Technologies web site in a new browser window.

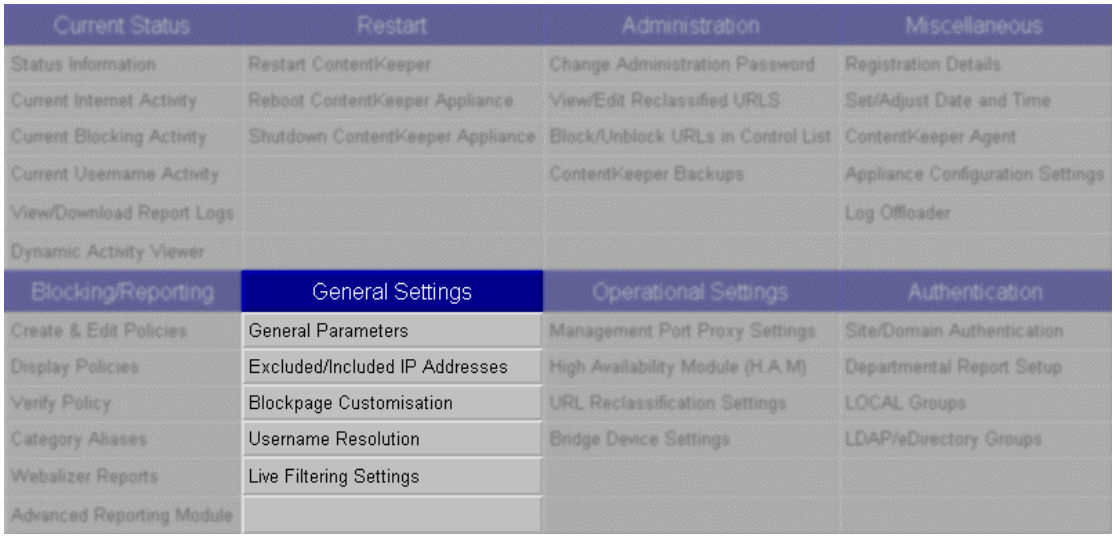
The ContentKeeper *Advanced Reporting Module* is a comprehensive enterprise level reporting package, which supports features such as template driven reporting and automated delivery of reports.

A separate user manual is provided for the ContentKeeper *Advanced Reporting Module*.

Note: Refer to the Reporting with ContentKeeper section in Chapter 4 for important information.

General Settings Menu

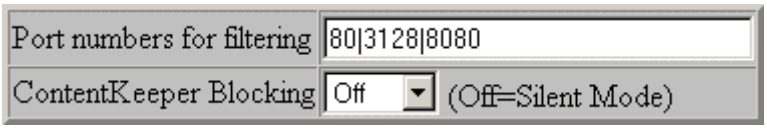
Items in the *General Settings* menu can be used to configure TCP ports for filtering, to enable or disable *Control List Blocking* and *Live Blocking*, to configure Excluded/Included IP address lists, to customise the ContentKeeper *blockpages*, and to configure *Username Resolution*.



General Parameters

Main Menu – General Settings → General Parameters

Select *General Parameters* from the *General Settings* menu to configure the global blocking controls for ContentKeeper. The settings in this menu override all other blocking settings within ContentKeeper. Selecting *General Parameters* from the *General Settings* menu to display the *General Parameters* table. Use the *General Parameters* table to enable or disable blocking and specify the ports on which ContentKeeper filter.



Note: Setting the *Block Web Pa*ges feature under the *General Parameters* menu to *Off* will disable all blocking by ContentKeeper. This is known as *Silent Mode*. Refer to the Silent Mode section in Chapter 4 for more information on using *Silent Mode*.

Port Numbers For Filtering

Use this setting to specify the TCP ports on which ContentKeeper will filter HTTP traffic. All entries into this field must be separated by a '|' pipe character, or ContentKeeper will ignore them.

Click the *Save* button after making changes to apply the new configuration to ContentKeeper.

Note: Refer to the *Network Topology* section in Chapter 3 for important information on specifying ports to filter when using a caching proxy server.

ContentKeeper Blocking

Important: This is the master blocking switch for ContentKeeper. Setting this to *Off* will prevent any *Block*, *Coach* or *Authenticate* pages from being displayed.

When this switch is set to *On*, ContentKeeper will operate in normal mode and produce *Block*, *Coach* or *Authenticate* pages whenever a policy requires them. When this switch is set to Off, ContentKeeper will operate in silent mode and will not produce *Block*, *Coach* or *Authenticate* pages. However, when operating in silent mode, ContentKeeper will still make entries into the *Current Internet Activity* and *Current Blocking Activity* logs based on policy settings.

Note: Refer to the Other Rules section in this chapter for more information on per-policy *blockpage* settings. Refer to the Silent Mode section in Chapter 4 for more information on using *Silent Mode*.

Excluded/Included IP Addresses

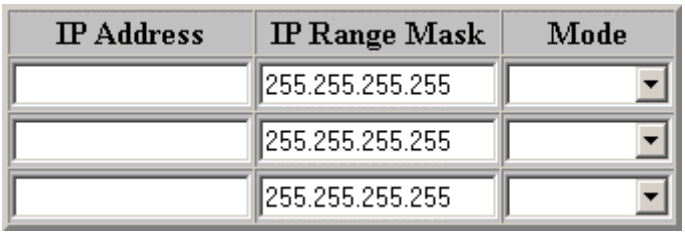
Main Menu – General Settings → Excluded/Included IP Addresses

Select *Excluded/Included IP Addresses* from the *General Settings* menu to define which IP addresses will and will not be filtered or blocked by ContentKeeper. Also use this menu to configure the *Catch All*.

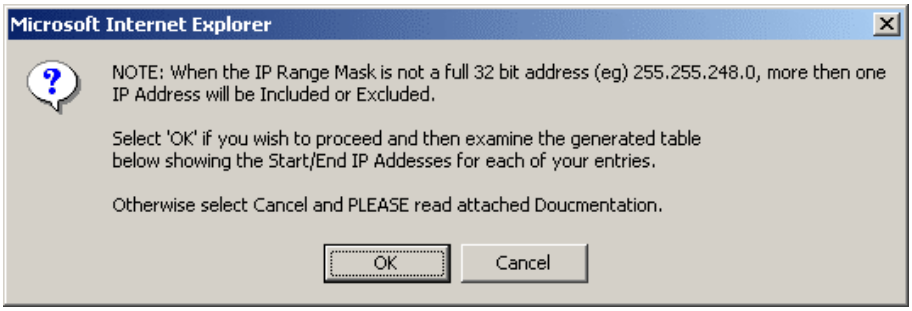
IP Address Table

Use a range mask to specify whether an IP address defined within the *Excluded/Included IP Addresses* table will represent a single address or a range of addresses. To specify one IP address only, use a range mask of 255.255.255.255.

Entries set to *Excluded* in the *Excluded/Included IP Addresses* table will not be filtered or blocked, and will therefore not appear in any Blocking Activity Reports.



Important: Ensure that the specified range mask is correct. Specifying a range mask of 255.255.255.0 when attempting to exclude or include a single IP address will result in a range of 255 IP addresses being excluded or included from filtering. In an attempt to prevent mis-configuration of the *Excluded/Included IP Addresses* menu, any time a range mask other than 255.255.255.255 is specified, the administrator will be asked to confirm the operation.


Microsoft Internet Explorer
NOTE: When the IP Range Mask is not a full 32 bit address (eg) 255.255.248.0, more then one IP Address will be Included or Excluded.
Select 'OK' if you wish to proceed and then examine the generated table below showing the Start/End IP Addesses for each of your entries.
Otherwise select Cancel and PLEASE read attached Doucmentation.
OK
Cancel

Catch All Mode

ContentKeeper employs a mechanism known as a *Catch All*. The Catch All has two modes, *Excluded* and *Included*. When in *Excluded* mode, blocking is not performed. When in *Included* mode, blocking is performed.

Use the *Catch All* to configure how ContentKeeper will process traffic destined to any IP address that is not defined in the *Excluded/Included IP Addresses* table.

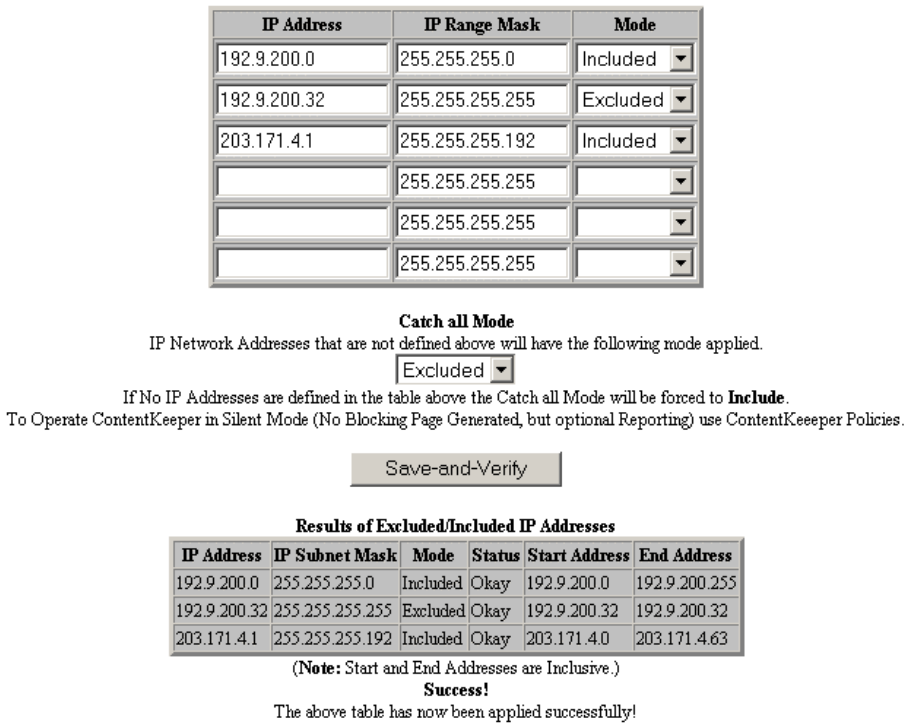
Note: If no IP addresses are defined in the *Excluded/Included IP Addresses* table, then the *Catch All* mode will be forced to *Include*.

The following table may be used as a guide when entering IP addresses.

Subnet Mask	No. IP Addresses In Range
255.255.0.0	65534
255.255.128.0	32766
255.255.192.0	16382
255.255.224.0	8190
255.255.240.0	4094
255.255.248.0	2046
255.255.252.0	1022
255.255.254.0	510
255.255.255.0	254
255.255.255.128	126
255.255.255.192	62
255.255.255.224	30
255.255.255.240	14
255.255.255.248	6
255.255.255.252	2
255.255.255.255	1

Save And Verify

Select *Save-and-Verify* to save any changes to the *Excluded/Included IP Addresses* table and display the current table so that all IP addresses and ranges may be verified.



IP Address	IP Range Mask	Mode
192.9.200.0	255.255.255.0	Included
192.9.200.32	255.255.255.255	Excluded
203.171.4.1	255.255.255.192	Included
	255.255.255.255	
	255.255.255.255	
	255.255.255.255	

Catch all Mode
IP Network Addresses that are not defined above will have the following mode applied.
Excluded
If No IP Addresses are defined in the table above the Catch all Mode will be forced to **Include**.
To Operate ContentKeeper in Silent Mode (No Blocking Page Generated, but optional Reporting) use ContentKeeeper Policies.

Save-and-Verify

Results of Excluded/Included IP Addresses

IP Address	IP Subnet Mask	Mode	Status	Start Address	End Address
192.9.200.0	255.255.255.0	Included	Okay	192.9.200.0	192.9.200.255
192.9.200.32	255.255.255.255	Excluded	Okay	192.9.200.32	192.9.200.32
203.171.4.1	255.255.255.192	Included	Okay	203.171.4.0	203.171.4.63

(**Note:** Start and End Addresses are Inclusive.)
Success!
The above table has now been applied successfully!

Example Excluded/Included IP Address Settings

The figure above depicts a populated *Excluded/Included IP Addresses* table. There are entries in the table that belong to two separate subnets, 192.9.200.0/255.255.255.0 and 203.171.4.0/255.255.255.192.

The following example is of the network from where the *Excluded/Included IP Addresses* table has been taken.

In this network, traffic belonging to both subnets passes through ContentKeeper on its way to and from the router. Note the following points:

- The administrator has configured ContentKeeper to include any traffic from the network address 192.9.200.0/255.255.255.0.
- The administrator has configured ContentKeeper to exclude any traffic from the host address 192. 9.200.32 from blocking.
- The administrator has configured ContentKeeper to include any traffic from the network address 203.171.4.0/255.255.255.192.
- The administrator has configured the *Catch All Mode* to Excluded, which means that blocking will not take place for any IP address not defined in the *Excluded/Included IP address* table and set to *Included*.

Blockpage Customisation

Main Menu – General Settings → Blockpage Customisation

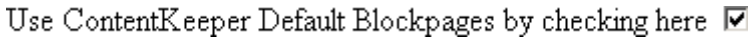
Select *Blockpage Customisation* from the *General Settings* menu to specify whether ContentKeeper will use the default blocking pages or customised blocking pages created by your local web master.

Customised *blockpages* are served up by a web server local to your network, e.g. your local Intranet server.

Note: This menu gives administrators access to examples of source code for customised *Block*, *Authenticate* and *Coach* pages. Refer to the Viewing Example Code section in this chapter for more information.

Enabling Customised Blockpages

Uncheck the *Use ContentKeeper Default Blockpages by checking here* check box to switch between the default and custom *blockpages*. Default *blockpages* are selected when the box is checked and the options below it are greyed out.



Configuring Customised Blockpages

Once you have enabled Customised Blockpages, you may configure them via the *Custom Blockpage Settings* table.

Specifying an HTTP Method

Select one of the two radio buttons in the *Custom Blockpage Settings* table to specify whether to process *Form Variables* in customised *blockpages* as HTTP *GET* or *POST* commands.

Specifying a Blockpage URL

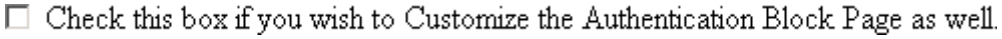
Enter the URL of your *customised blockpage* into the input field to the right of the HTTP method radio buttons. This URL, or network path, is usually a web address consisting of the IP address or DNS name of the server where your *customised blockpage* resides, and the path on the server to the *customised blockpage*.

Note: When entering a *customised blockpage* URL it is not necessary to enter the URL for both HTTP methods.

Customising the Authenticate Blockpage

By default ContentKeeper does not support customisation of the *Authenticate blockpage*. If you wish to customise the *Authenticate blockpage* as well as the standard *Block* and *Coach blockpages*, you must configure ContentKeeper to support this and pass the necessary information to the *Custom Blockpage*.

To enable customisation of the *Authenticate blockpage*, place a check in the *Check this box if you wish to Customize the Authentication Block Page as well* check box below the *Custom Blockpage Settings* table.



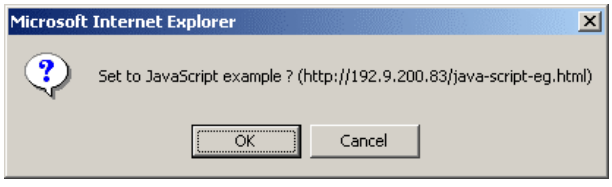
Viewing Example Code

ContentKeeper comes with a number of *Custom Blockpage* source code examples. These examples may be viewed by clicking on either of the *View Example* buttons in the *Custom Blockpage Settings* table, or by clicking the *Coldfusion* hyperlink at the bottom of the *Blockpage Customisation* menu.

Example JavaScript Code

Click the *View Example* button in the top section of the *Custom Blockpage Settings* table to view the example JavaScript code.

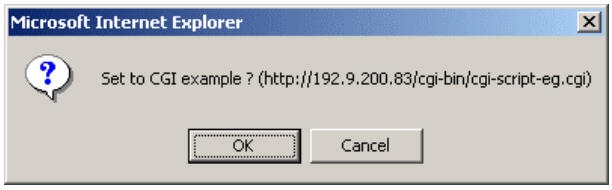
Click the *A Jscript Example* button in the top section of the *Custom Blockpage Settings* table to set the default *Custom Blockpage* test type to JavaScript. You will be prompted to confirm your actions.



Example CGI Code

Click the *View Example* button in the bottom section of the *Custom Blockpage Settings* table to view the example CGI code.

Click the *A CGI Example* button in the top section of the *Custom Blockpage Settings* table to set the default *Custom Blockpage* test type to CGI. You will be prompted to confirm your actions.



Example Coldfusion Code

Click the *Coldfusion* hyperlink at the bottom of the *Blockpage Customisation* menu to view the example *Coldfusion* code.

The default *Custom Blockpage* test type cannot be set to *Coldfusion*.

Save button

Click the *Save and Redisplay* button to apply the configuration changes to ContentKeeper.

Note: Applying configuration changes to ContentKeeper with the default values for either of the example *custom blockpages* in the *Custom Blockpage Settings* table will result in non-standard blockpages being generated by ContentKeeper. If you are not using *custom blockpages*, ensure that you disable them, and then click *Save and Redisplay* before leaving the menu.

Testing Custom Blockpages

Enter a URL from a *Category* that is set to *Block* or a *Custom URL* that is defined as *Blocked* then, select a test type and click the *Test* button to view the example custom Blockpage.

Note: You must be browsing from a workstation that is being filtered by ContentKeeper for this test to work.

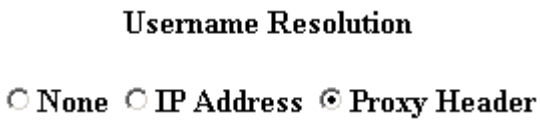
Username Resolution

Main Menu – General Settings → Username Resolution

Important: ContentKeeper reports and policies rely on *Username Resolution* to operate correctly.

ContentKeeper supports three main modes of *Username Resolution*; these are *None*, *IP Address* and *Proxy Header*. Each mode uses different methods to resolve URL requests to usernames. Use the following sections to help you select the method that is most suitable to your network.

Note: Some of the options presented here must be accessed through the *Username Resolution Advanced Settings* menu. This will be indicated where appropriate. To access the *Username Resolution Advanced Settings* menu, select *Username Resolution* from the *General Settings* menu, and then click the *Advanced Settings* button.



Available Username Resolution Methods

To properly configure the method of name resolution you must first know which methods are available within your network. Using this information to choose a *Username Resolution* method is discussed in the Choosing a Username Resolution Method section in Chapter 4.

Once you have determined which *Username Resolution* methods are available on your network, can use this information to configure ContentKeeper's method of *Username Resolution*.

None

When *Username Resolution* is set to *None*, no *Username Resolution* will be performed and only an IP address will be associated with a URL request. The implications of using this setting are:

- Only IP addresses will appear in ContentKeeper reports.
- Only policies that are configured with IP addresses will be applied. If ContentKeeper cannot resolve usernames then it cannot match URL requests to usernames in policies.

To configure ContentKeeper to use a *Username Resolution* method of *None*, select the *None* radio button at the top of the *Username Resolution* menu and click the *Save* button.

IP Address

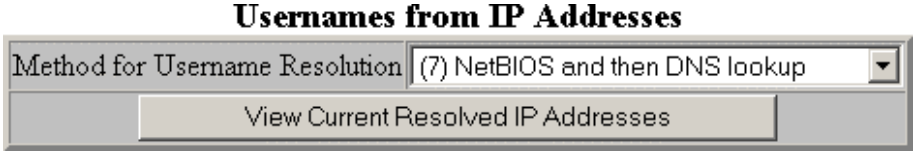
When *Username Resolution* is set to *IP Address*, ContentKeeper will use DNS, NetBIOS, IDENT, eDirectory or a combination of any two to resolve URL requests to hostnames and usernames. Any of the IP Address *Username Resolution* methods may also be combined with the *Auto Proxy Username Resolution* method. Refer to the Proxy Header section in this chapter for more information about the *Auto Proxy Username Resolution* method.

Note: The *Management Port* performs *IP Address Username Resolution*; therefore the location of the *Management Port* relevant to the network clients (user workstations) is important. Refer to the ContentKeeper Management Port Location section in Chapter 2 for more information.

Method For Username Resolution

To configure *IP Address Username Resolution*, first select the *IP Address* radio button at the top of the *Username Resolution* menu, and then select a single method or a method combination from the *Method for Username Resolution* drop-down in the *Usernames from IP Addresses* table. Finally, click the *Save* button.

Each of the available *IP Address Username Resolution* methods is explained below.


Usernames from IP Addresses
Method for Username Resolution
(7) NetBIOS and then DNS lookup
View Current Resolved IP Addresses

DNS Lookup

The *DNS Lookup Username Resolution* method relies on a DNS server being available on the network that the *Management Port* is attached to. ContentKeeper will use the DNS server that the *Management Port* was configured with to resolve usernames.

If a DNS query is successful the requesting IP address will be resolved to *hostname.domain* or just *hostname*, depending on the settings in the *Advanced Settings* menu.

NetBIOS Lookup

The *NetBIOS Lookup Username Resolution* method involves the *Management Port* performing a NetBIOS over TCP/IP (NetBT) query the requesting IP address.

If a NetBIOS query is successful the IP address will be resolved to *username@biosname* or just *username*, depending on the settings in the *Advanced Settings* menu.

IDENT-AUTH Lookup

The *IDENT-AUTH Lookup Username Resolution* method relies on an IDENT server running on the network clients (user workstations). The *Management Port* performs an IDENT query to the requesting IP address.

If an *IDENT-AUTH* query is successful the IP address will be resolved to *username*.

Note: There are many IDENT servers for the Windows® operating system freely available on the Internet.

eDirectory Lookup

The *eDirectory Lookup Username Resolution* method involves the *Management Port* performing an LDAP query to a specified eDirectory (NDS) server.

If an *eDirectory Lookup* query is successful the IP address will be resolved to *username*.

Note: eDirectory server settings may be configured through the *Advanced Settings* menu. Refer to the eDirectory Settings section in this chapter for more information.

View Current Resolved IP Addresses

Click on the *View Current Resolved IP Addresses* button to display a list of the currently resolved IP addresses and their associated usernames.

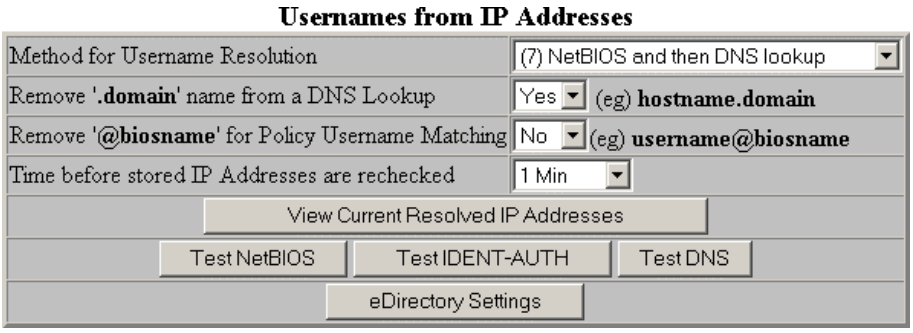
Current list of Resolved IP Addresses

No.	IP Address	Result	Time IP Address Resolved
1	192.9.200.195	perle833is-dialin-pool-2	24-09-2002; 13:07:27
2	192.9.200.243	administrator@elimatta	24-09-2002; 13:10:10
3	10.0.0.2	www	24-09-2002; 13:09:16
4	172.16.0.2	mail	24-09-2002; 13:09:30
5	192.9.200.4	paul@gateway	24-09-2002; 13:09:46
6	192.9.200.5	administrator@dev	24-09-2002; 13:09:48
7	192.9.200.9	administrator@rpa-2	24-09-2002; 13:09:38
8	192.9.200.10	sysmonitor	24-09-2002; 13:09:51
9	192.9.200.13	bigpond	24-09-2002; 13:10:45
10	192.9.200.15	mark@peru	24-09-2002; 13:09:42

Advanced Settings

The *Username Resolution Advanced Settings* menu may be accessed from the *Username Resolution Basic Settings* menu by clicking on the *Advanced Settings* button at the bottom of the screen.

Use the *Advanced Settings* menu to customise your *Username Resolution* method. There are four features to customise here: method, removal of domain name, removal of BIOSname and recheck frequency. Each feature is described below.



Method

Refer to the Method for Username Resolution section in this chapter for more information on choosing a method for *Username Resolution*.

Remove Domain Name From DNS Lookup

Select *Yes* or *No* from the *Remove Domain Name From DNS Lookup* drop-down to enable or disable this option. When enabled, ContentKeeper will remove the domain name from the DNS name returned during *Username Resolution*, and IP addresses will be resolved to *hostname*. When disabled, ContentKeeper will resolve IP addresses to *hostname.domain*.

Enabling this option allows ContentKeeper policies to target specific users, ignoring domain names. This option does affect reporting where the domain name may not always be displayed.

Remove @biosname For Policy Username Matching

Select *Yes* or *No* from the *Remove @biosname For Policy Username Matching* drop-down to enable or disable this option. When enabled, ContentKeeper will remove the biosname name from the NetBIOS name returned during *Username Resolution*. When disabled, ContentKeeper will resolve IP addresses to *username@biosname*.

Enabling this option allows ContentKeeper policies to target specific users, ignoring machine names (biosnames). This option does not affect reporting where the machine name is always displayed.

Time Before Stored IP Addresses Are Rechecked

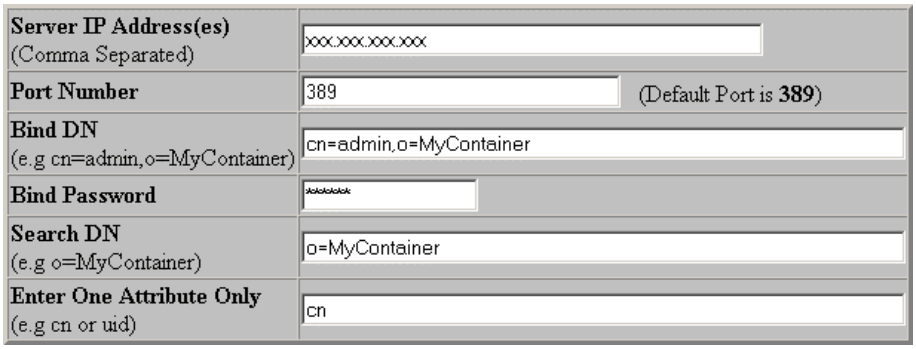
Use this setting to configure how long resolved IP addresses are considered to be valid by selecting a value between five minutes and twenty-four hours from the *Time before stored IP Addresses are rechecked* drop-down. Once the specified time period expires for any IP address, ContentKeeper will again attempt to resolve that IP address to a username.

View IP Addresses

Refer to the View Current Resolved IP Addresses section in this chapter for more information on viewing the currently resolved IP addresses.

eDirectory Settings

Use the *eDirectory Settings* table to configure communications between ContentKeeper and a remote eDirectory server. The *eDirectory Settings* table consists of a number of server parameter fields, each of which is explained below.



Server IP Address(es)

Enter the IP address of your eDirectory server into the *Server IP Address(es)* input field in the form of xxx.xxx.xxx.xxx. Do not specify a subnet mask. Multiple IP addresses may be specified if you have multiple eDirectory servers, each separated by a semi-colon.

Port Number(s)

Enter the port number into the *Port Number(s)* input field on which ContentKeeper is to connect to the eDirectory server. Multiple port numbers may be specified, each separated by a pipe character '|'. The default port number is 389.

Bind DN

Enter the bind DN (Distinguished Name) into the *Bind DN* input field. Multiple container names may be specified, each separated by a comma. The information specified in the *Bind DN* input field will be used by ContentKeeper when authenticating to the eDirectory server.

Bind Password

Enter the password used to authenticate and bind to the LDAP directory into the *Bind Password* input field. This information is used by ContentKeeper in conjunction with the information specified in the *Bind DN* input field.

Search DN

Enter the container, or point, in the directory from which to begin the search for your organisations users. Typically this will be an *o* (organisation) or *ou* (organisational unit).

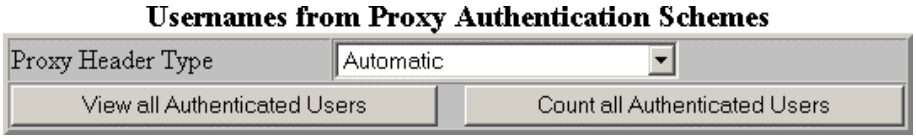
Enter One Attribute Only

Enter the object that you would like the search to return, into the *Enter One Attribute Only* input field. This object should contain the users unique username, i.e. the username with which the user authenticates to a proxy server or the LDAP directory with when accessing the Internet. Typically this will be a cn (common name) or a uid (unique identifier).

Proxy Header

This method of *Username Resolution* is designed to work when your network clients (user workstations) connect to the Internet through a caching proxy server that requires user authentication. In this configuration the *ContentKeeper Bridge* is placed between the network clients and the proxy server. The proxy server must be configured to use either a non-proprietary, IETF based, authentication scheme, or Microsoft's NTLM authentication scheme

Note: You may wish to use *Proxy Header* username resolution in conjunction with *NT Security Groups* directory service in a policy. In this case, the location of the management port is relevant. Refer to ContentKeeper Agent section in this chapter for more information.



Proxy Header Type

To configure *Proxy Header Username Resolution*, first select the *Proxy Header* radio button at the top of the *Username Resolution* menu, and then select a proxy header type that matches that used by your proxy server from the *Proxy Header Type* drop-down in the *Usernames from Proxy Authentication Schemes* table. Finally, click the *Save* button.

Each of the available *Proxy Header Username Resolution* methods is explained below.

Basic Authentication Scheme

Choose *Basic Authentication Scheme* as the *Proxy Header Type* when a non-proprietary, IETF based, proxy authentication method is being used.

Note: Refer to the IETF web site, http://www.ietf.org/ for more details on the basic proxy authentication scheme.

NTLM Authentication Scheme

Choose *NTLM Authentication Scheme* as the *Proxy Header Type* when a Microsoft Proxy or Internet Security & Acceleration (ISA) server is being used as the proxy server on your network, and has Authentication enabled. Choose *NTLM Authentication Scheme* when the following conditions are met.

- When a *Microsoft Proxy Server* is being used with NTLM as the authentication type, ContentKeeper will successfully perform username resolution on HTTP traffic bound for the proxy server.

- When a *Microsoft ISA Server* is being used with Integrated Authentication as the authentication type, ContentKeeper will successfully perform username resolution on HTTP traffic bound for the proxy server.

Digest Authentication Scheme

Choose *Digest Authentication Scheme* as the *Proxy Header Type* when the Digest proxy authentication method is being used.

Automatic

Choose *Automatic* as the *Proxy Header Type* to allow ContentKeeper to automatically detect the *Proxy Authentication Scheme*. ContentKeeper supports the automatic detection of the following authentication schemes:

- Basic
- NTLM
- Digest

The *Automatic* proxy header *Username Resolution* method is useful when your proxy server employs more than one authentication scheme, or you have more than one proxy server, each employing different authentication schemes

View All Authenticated Users

Click on the *View All Authenticated Users* button at the bottom of the *Usernames from Proxy Authentication Schemes* table to display a list of the currently resolved proxy users.

List of Collected Proxy Users

No.	Username	Time of Last Request
1	matthew	08-Sep-2002,19:37
2	paulp	08-Sep-2002,18:30
3	peter	08-Sep-2002,16:59
4	timh	08-Sep-2002,15:08
5	mario	08-Sep-2002,13:26
6	paulpatti	08-Sep-2002,13:23
7	aaron	08-Sep-2002,11:39
8	david	07-Sep-2002,17:00
9	mark	07-Sep-2002,09:23
10	admin	06-Sep-2002,18:10
11	tim	06-Sep-2002,17:03
12	paul	06-Sep-2002,16:57
13	antony	06-Sep-2002,16:37
14	hannah	06-Sep-2002,15:00
15	debbie	06-Sep-2002,14:41
16	DEBBIE	05-Sep-2002,10:07
17	fabian	04-Sep-2002,18:50
18	johnm	04-Sep-2002,11:14

Count All Authenticated Users

Click on the *Count All Authenticated Users* button at the bottom of the *Usernames from Proxy Authentication Schemes* table to display the total number of currently resolved proxy users.

NT Domain Names

The *NT Domain Names* section, accessible from the *Advanced Username Resolution* menu, presents the option to remove the domain name component from a resolved username for username matching. This prevents the need to enter a domain name when configuring policies.

The option to remove the domain name component applies to usernames resolved under the *NTLM Authentication Scheme*, as well as usernames supplied to ContentKeeper by the ContentKeeper Agent. Usernames obtained by either of these methods are in the form of *Username/NTDomain*, where

Username is the name of a user and *NTDomain* is the name of the Windows NT domain to which that user belongs.

When enabled, this option will cause ContentKeeper to remove the /NTDomain component prior to attempting to match a username to a policy directory object.

Note: Refer to the Select Your Directory Service section in Chapter 4 for more information.

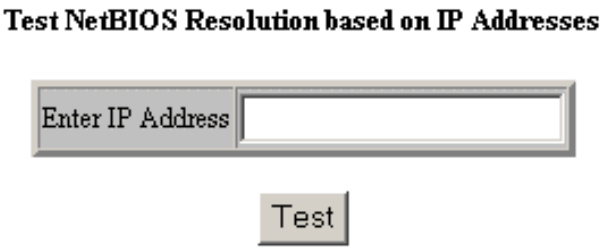
This option is particularly useful when ContentKeeper is operating in an environment that has only one Windows NT or Windows 2000 domain, and as such there is no need to distinguish between members of different domains.

Testing Username Resolution

ContentKeeper provides facilities for testing all *IP Address Username Resolution* methods. *Username Resolution* testing facilities may be accessed from the *Advanced Settings* menu.

Test NetBIOS Resolution

To test *NetBIOS* resolution with ContentKeeper, click on the *Test NetBIOS* button in the *Advanced Settings* menu. A new window will open containing a facility for testing *NetBIOS* name resolution.



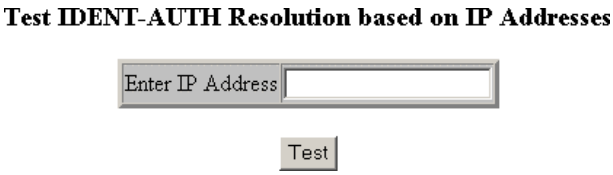
To use the *NetBIOS* test facility, enter an IP address or range of IP addresses into the *Enter IP Address* input field, then click the *Test* button. IP address ranges may be entered by specifying the start and finish of the range, or by specifying a bitmask.

BitMask - To specify an IP address range with a bitmask, enter IP address, slash, and bitmask. For example, entering 192.9.200.0/24 will cause all 256 IP addresses in the range 192.9.200.0 to 192.9.200.255 to be resolved.

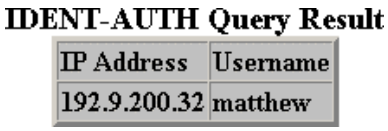
Address Range - Enter an IP address range by specifying the start and finish addresses. For example, entering 192.9.200.2-60 will cause all 59 IP addresses in the range 192.9.200.2 to 192.9.200.60 to be resolved.

Test IDENT-AUTH Resolution

To test *IDENT-AUTH* resolution with ContentKeeper, click on the *Test IDENT-AUTH* button in the *Advanced Settings* menu. A new window will open containing a facility for testing *IDENT-AUTH* name resolution.

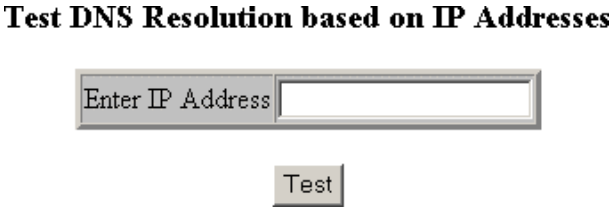


To use the *IDENT-AUTH* test facility, enter an IP address into the *Enter IP Address* input field, then click the *Test* button. IP address ranges may not be entered.

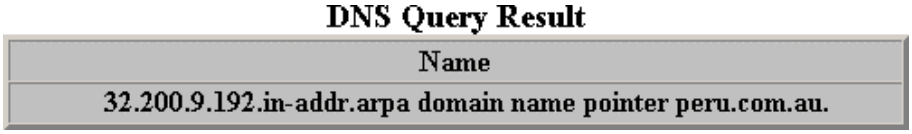


Test DNS

To test *DNS* resolution with ContentKeeper, click on the *Test DNS* button in the *Advanced Settings* menu. A new window will open containing a facility for testing *DNS* name resolution.

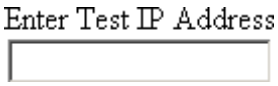


To use the *DNS* test facility, enter an IP address into the *Enter IP Address* input field, then click the *Test* button. IP address ranges may not be entered.



Test eDirectory

To test *eDirectory* resolution with ContentKeeper, click on the *eDirectory Settings* button in the *Advanced* S*ettings* menu. A new window will open containing the *eDirectory Settings* table. A facility for testing *eDirectory* name resolution may be found below the *eDirectory Settings* table.



To use the *eDirectory* test facility, enter an IP address into the *Enter Test IP Address* input field, then click the *Test, Save and Redisplay* button. IP address ranges may not be entered.

Live Filtering Settings

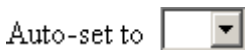
Main Menu – General Parameters → Live Filtering Settings

Use this menu to manage *ContentKeeper Live Filtering.* From this menu *Live Filtering* may be configured on a per *Category* basis, and the *Live Filtering* language settings may be configured. Select *Live Filtering Settings* from the *General Parameters* menu to display a table of all *Categories*.

Index	Category	Live Block State	Index	Category	Live Block State
1	Adult Content	☑	17	www-Email Sites	☑
2	News	☑	18	Violence/Undesirable	☑
3	Job Search	☑	19	Malicious	☑
4	Gambling	☑	20	Search Sites	☑
5	Travel/Tourism	☑	21	Health Sites	☑
6	Shopping	☑	22	Clubs and Societies	☑
7	Entertainment	☑	23	Music Downloads	☑
8	Chatrooms	☑	24	Business Oriented	☑
9	Dating Sites	☑	25	Government Blocking List	☐
10	Game Sites	☑	26	Educational	☑
11	Investment Sites	☑	27	Advertising	☑
12	E-Banking	☑	28	Drugs/Alcohol	☑
13	Crime/Terrorism	☑	29	Computing/IT	☑
14	Personal Beliefs/Cults	☑	30	Swimsuit/Lingerie/Models	☑
15	Politics	☑	31	Reserved	☑
16	Sports	☑	32	Reserved	☑

Setting a *Category* to *On* will cause ContentKeeper to include that *Category* when live filtering.

Clicking on a checkbox (☐) will place a tick in it (☑), setting the *Category* to *On*; alternatively the Auto-set feature may be used to automatically set all *Categories* to either *On* or *Off*.

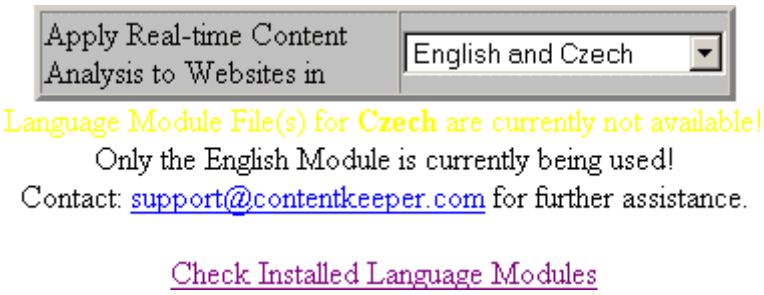


Live Filtering Aggressiveness

Use the *Live Filtering Aggressiveness* table to adjust the aggressiveness of ContentKeepers *Live Filtering* engines. This feature can be useful if you find that ContentKeeper is being too aggressive in its *Live Filtering*.

Live Filtering Language Settings

Use the *Live Filtering Language Settings* table to configure which languages *Live Filtering* is performed in. By default *Live Filtering* is performed in English only, however you may configure to perform *Live Filtering* in English and one other language simultaneously by selecting the desired language combination from the drop-down in the *Live Filtering Language Settings* table.


Apply Real-time Content Analysis to Websites in
English and Czech
Language Module File(s) for Czech are currently not available!
Only the English Module is currently being used!
Contact: support@contentkeeper.com for further assistance.
Check Installed Language Modules

Checking Installed Modules

ContentKeeper must have the appropriate *Language Module* installed to perform *Live Filtering* in languages other than English. If a language combination is selected for which the *Language File* is not installed, then an error message will be displayed below the *Live Filtering Language Settings* table warning of the missing *Language File*. In this case, contact ContentKeeper technical support for assistance.

Note: Refer to the Obtaining Technical Support section in the Introduction for more information about contacting ContentKeeper technical support.

You may check which *Language Modules* are installed on your ContentKeeper appliance by clicking the *Check Installed Language Modules* hyperlink at the bottom of the *Live Filtering Settings* menu, which will cause the *Language Module Status* table to be displayed in a new browser window.

Encoded/Compressed Language Modules Status

#	Language	Module 1	CRC	Module 2	CRC
0	English	**Avaliable**	9680	**Avaliable**	14736
1	French				
2	German				
3	Italian				
4	Spanish				
5	Danish				
6	Dutch				
7	Greek				
8	Thai				
9	Portugese				
10	Czech				

The *Language Module Status* table consists of six columns, each of which is defined below:

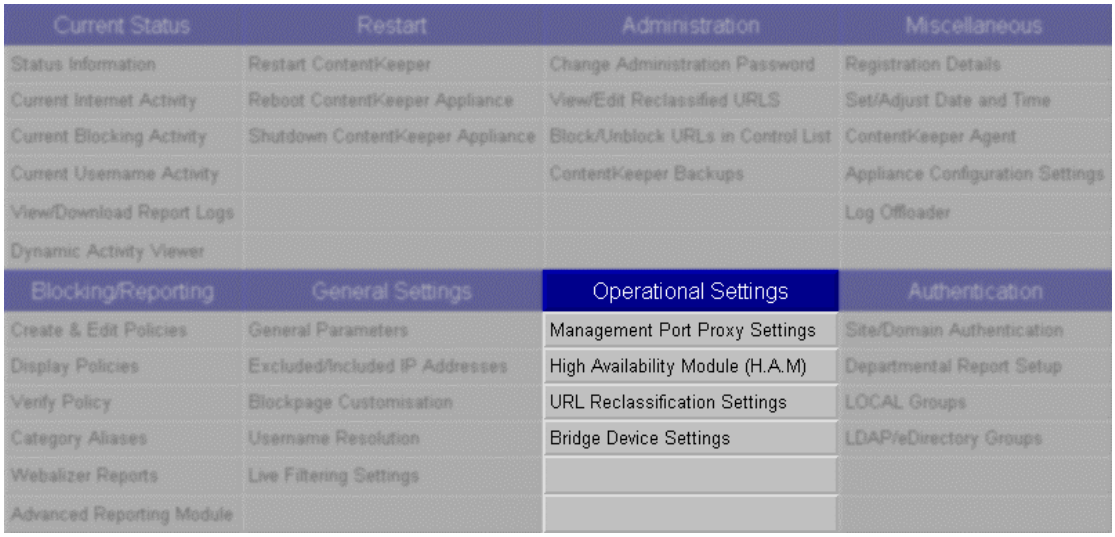
- # **(Index)** – The *Index* column contains an index of each *Language Module* entry for easy reference.
- **Language** – The *Language* column contains a list of the supported languages.
- **Module 1** – The *Module 1* column contains the status of the first module for each language. If the module is installed the word *Available* will appear in this column, otherwise the column will be empty.
- **CRC** – The first *CRC* column contains the CRC value of module one for each language. The value in this column is the result of a check of the modules validity. A number, or CRC, indicates that the module is valid. An *Error* message indicates that the module is invalid and may be corrupt. In this case, contact ContentKeeper technical support for assistance.
- **Moduke 2** – The *Module 2* column contains the status of the second module for each language. If the module is installed the word *Available* will appear in this column, otherwise the column will be empty.
- **CRC** – The second *CRC* column contains the CRC value of module two for each language. The value in this column is the result of a check of the modules validity. A number, or CRC, indicates that the module is valid. An *Error* message indicates that the module is invalid and may be corrupt. In this case, contact ContentKeeper technical support for assistance.

Save and Redisplay

Click the *Save and Redisplay* button after making changes to apply the new configuration to ContentKeeper.

Operational Settings Menu

Items in the *Operational Settings* menu allow you to configure *Management Port Proxy Settings*, the *High Availability Module*, *URL Reclassification Settings* and *Bridge Device Settings*.



Management Port Proxy Settings

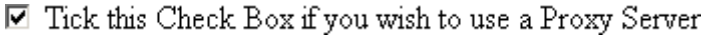
Main Menu – Operational Settings → Management Port Proxy Settings

Select *Management Port Proxy Settings* from the *Operational Settings* menu to enable or disable the use of a proxy server by the *Management Port* when obtaining hourly *URL Database* updates from the *ContentKeeper DataCenter*. Through this menu you may specify a proxy server IP address and port, as well as a username and password if your proxy server requires authentication.

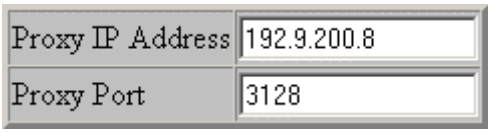
Note: If the ContentKeeper *Management Port* has been configured to connect to the *DataCenter* through a proxy server, but is unable to do so, it will attempt to connect directly through its network gateway.

Proxy Server Settings

To enable the *Management Port* to use a web cache proxy server when connecting to the *ContentKeeper DataCenter* you must first place a tick in the check box above the *Proxy Server Settings* table.



Only once a tick has been placed in the check box above the *Proxy Server Settings* table will the *Proxy Server Settings* table become available. Once this is done, you may specify your proxy server settings.



Proxy IP Address

Enter the IP address of the proxy server you would like ContentKeeper to use, in the form of xxx.xxx.xxx.xxx, into the *Proxy IP Address* input field. Do not specify a subnet mask.

Proxy Port

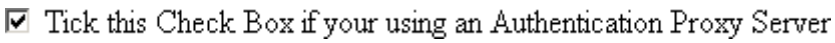
Enter the port number on which your proxy server is set to listen for HTTP traffic. ContentKeeper will use this information to communicate with the proxy server.

Note: You must click the *Save and Restart* button to apply the settings to ContentKeeper.

Authentication Settings

ContentKeeper will only authenticate to a web cache proxy server using the Basic authentication scheme, thus if you wish ContentKeeper to authenticate to your proxy server, it must support and be configured to offer the Basic authentication scheme. Your proxy server may also be configured to offer other authentication schemes such as NTLM (or Integrated) and Digest.

To enable the *Management Port* to authenticate to a web cache proxy server when connecting to the *ContentKeeper DataCenter* you must first place a tick in the check box above the *Authentication Settings* table.



Only once a tick has been placed in the check box above the *Authentication Settings* table will the *Authentication Settings* table become available. Once this is done, you may specify your authentication settings.

Username

Enter the username with which ContentKeeper will authenticate to your proxy server into the *Username* input field. Usernames must be a maximum of thirty-two characters in length.

If you are authenticating to a Microsoft Proxy or ISA server, or any web cache proxy server that offers NTLM authentication, you may have to specify a domain name with the username in the form of *DomainName******Username*.

Password

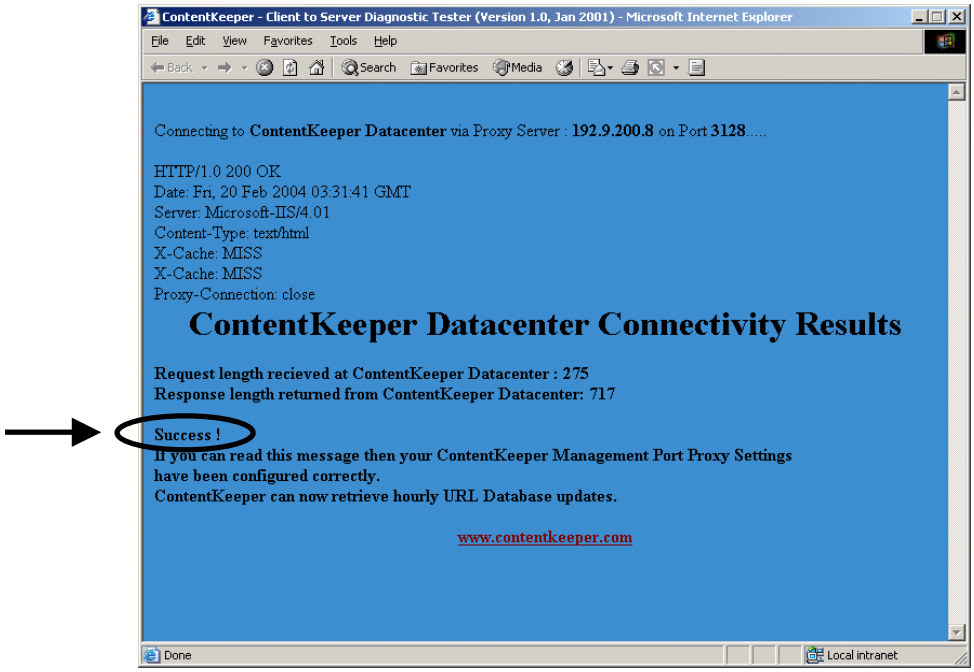
Enter the password with which ContentKeeper will authenticate to your proxy server into the *Password* input field. Passwords must be a maximum of thirty-two characters in length.

Note: You must click the *Save and Restart* button to apply you settings to ContentKeeper.

Testing Connectivity

ContentKeeper provides a facility for you to test your proxy server settings in the form of a *Save and Test Only* button at the bottom of the *Management Port Proxy Settings* menu.

Once you have specified a proxy server IP address and port number, and optionally specified a username and password, you may click the *Save and Test Only* button to test your new settings. The results will be displayed in a new browser window. A blue results screen with the word *Success !* on it, similar to the one on the following page, indicates a successful test.


ContentKeeper - Client to Server Diagnostic Tester (Version 1.0, Jan 2001) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Connecting to ContentKeeper Datacenter via Proxy Server : 192.9.200.8 on Port 3128.....
HTTP/1.0 200 OK
Date: Fri, 20 Feb 2004 03:31:41 GMT
Server: Microsoft-IIS/4.01
Content-Type: text/html
X-Cache: MISS
X-Cache: MISS
Proxy-Connection: close
ContentKeeper Datacenter Connectivity Results
Request length recieved at ContentKeeper Datacenter : 275
Response length returned from ContentKeeper Datacenter: 717
Success !
If you can read this message then your ContentKeeper Management Port Proxy Settings have been configured correctly.
ContentKeeper can now retrieve hourly URL Database updates.
www.contentkeeper.com
Done
Local intranet

If the test fails, the reason will be displayed in the new browser window.

Note: You must click the *Save and Restart* button to apply you settings to ContentKeeper.

High Availability Module (H.A.M)

Main Menu – Operational Settings → High Availability Module (H.A.M)

Select *High Availability Module (H.A.M)* from the *Operational Settings* menu to configure the ContentKeeper *High Availability Module*.

Note: For an introduction to the *High Availability Module*, and information on installing it, refer to the section High Availability Module (H.A.M) in Chapter 2.

The H.A.M Settings Table

Use the *H.A.M Settings* table to configure ContentKeeper to use the *H.A.M*.

H.A.M Settings for an Internal Device.
(Firmware Version : **1.10**)

Parameter	Value
Mode	On
Enable Buzzer (When in ByPass)	Yes
Ignore UTP Gigabit Heartbeat	Yes

Mode

Use the *Mode* parameter to enable or disable the *H.A.M*. Selecting either *On* or *Off* from the *Mode* drop-down will enable or disable the *H.A.M* respectively.

Disabling the *H.A.M* will force it into *Bypass* mode. If ContentKeeper is connected to the network via the *H.A.M* when it is disabled then no further traffic will traverse the ContentKeeper *Bridge Ports* until the *H.A.M* is removed from circuit i.e. the network cables are plugged straight into the ContentKeeper *Bridge Ports*, or the *H.A.M* is re-enabled.

Enable Buzzer

Use the *Enable Buzzer* parameter to enable or disable the *H.A.M* warning buzzer. Selecting either *On* or *Off* from the *Enable Buzzer* drop-down will enable or disable the *H.A.M* warning buzzer respectively.

The *H.A.M* warning buzzer will sound with a beep at five second intervals when the *H.A.M* is forced into *Bypass* mode, or if ContentKeeper stops responding. The warning buzzer is located inside the *H.A.M* and therefore does not sound on a workstation with a browser connected to the *Web Interface*.

Ignore UTP Gigabit Heartbeat

If your ContentKeeper appliance uses auto-polarity sensing Gigabit UTP ports for the *Bridge Ports*, then these ports do not produce Ethernet heartbeat and ContentKeeper must be configured not to look for it.

Use the *Ignore UTP Gigabit Heartbeat* parameter to enable or disable monitoring of UTP heartbeat. Selecting either *On* or *Off* from the *Ignore UTP Gigabit Heartbeat* drop-down will enable or disable monitoring of UTP heartbeat respectively.

Save

You must click the *Save* button to apply your settings to ContentKeeper, before they will take effect. Clicking the *Save* button will cause the ContentKeeper processes to restart.

Managing the H.A.M

Use the buttons at the bottom of the *High Availability Module (H.A.M)* menu to force the *H.A.M* into *Online* or *Bypass* mode, to acknowledge the alarm (buzzer), and to query the status of the *H.A.M*.

Force Bypass Mode

Click on the *Force Bypass Mode* button to force the *H.A.M* into *Bypass* mode and hence force Ethernet traffic to bypass ContentKeeper. ContentKeeper will not filter Ethernet traffic while the H.A.M. is in *Bypass* mode.

Force Online Mode

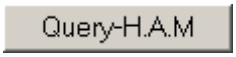
Click on the *Force Online Mode* button to force the *H.A.M* into *Online* mode, and hence force Ethernet traffic through the ContentKeeper *Bridge Ports*.

Acknowledge Alarm

Click on the *Acknowledge Alarm* button to turn off the *H.A.M* warning alarm (buzzer). Doing this does not restore any lost connections.

Query H.A.M

Click on the *Query H.A.M* button to test connectivity between ContentKeeper and the *H.A.M* and to confirm *H.A.M* configuration changes.



If ContentKeeper and the *H.A.M* have been set up correctly then the *Current State* table will be displayed listing *Operational Mode* as *Online* and all ports as *On*.

Current State.

Operational Mode	**Online**
Internet Connection	**On**
Enterprise Lan Connection	**On**
Bridge Port 1	**On**
Bridge Port 2	**On**

Cause Codes and Uptime

H.A.M cause codes can be useful in diagnosing *H.A.M* issues and network connectivity issues.

When the *H.A.M* is queried, the *Current Cause Codes* and *H.A.M Uptime* are returned at the bottom of the *Current State* table. Cause codes indicate how and why the *H.A.M* has changed state from *Online* to *Bypass* mode and vice versa. The *H.A.M Uptime* is how long the *H.A.M* has been operational. This time counter is reset if ContentKeeper is reset.

Current Cause Codes.
BYPASS 00 = No ONLINE to BYPASS Transition Yet.
ONLINE 01 = Forced ONLINE.

H.A.M Uptime.
1:08:32

View Status Log

Click on the View Status Log button to view the *H.A.M* status log file.

This *H.A.M* status log file will include the following information:

- The serial port to which the H.A.M. is attached
- The H.A.M. BIOS revision
- The date and time which the H.A.M. was activated
- H.A.M. mode (monitoring and timer)
- Buzzer mode
- Ethernet auto-negotiation mode
- The result of any query to the H.A.M.
- Any error messages from the H.A.M. or ContentKeeper

Configuring the H.A.M

Important: Do not attempt to configure ContentKeeper to use the H.A.M unless it is physically present and attached to ContentKeeper. Doing so will result in an error message from ContentKeeper.

Use the following procedure to configure ContentKeeper to use the *H.A.M*.

1. Select *High Availability Module (H.A.M.)* from the *Operational Settings* menu then select *On* from the *Mode* drop-down to enable the *H.A.M*.

Note: If the *H.A.M* mode is set to *Off* in this menu and a *H.A.M* is being used with ContentKeeper, all traffic will bypass the ContentKeeper applaince and no filtering will take place.

2. Select either *Yes* or *No* from the *Enable Buzzer* drop-down to either enable or disable *H.A.M Bypass* mode warning alarm.

3. Click *Save* to apply the new settings to ContentKeeper.

4. Confirm the success of the operation by clicking on the *Query H.A.M* button and reviewing the results.

ContentKeeper is now configured to use the *H.A.M*. The Ham status will appear on the console screen, as well as at the top of the *Status Information* menu.

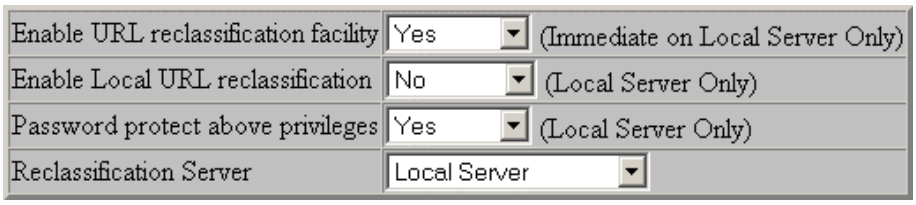
URL Reclassification Settings

Main Menu – Operational Settings → URL Reclassification Settings

Select *URL Reclassification Settings* from the *Operational Settings* menu to configure URL reclassification for your ContentKeeper appliance. It is essential that the ContentKeeper URL reclassification facility be configured correctly. URL reclassification settings determine how the local ContentKeeper appliance processes URL reclassification requests, as well as the degree to which your ContentKeeper site participates in the *Closed Loop Collaborative Filtering*™ process.

Configuring URL Reclassification

Use the URL Reclassification Settings table to configure URL reclassification for ContentKeeper.



Enable URL Reclassification Facility

Select *Yes* or *No* from the *Enable URL Reclassification Facility* drop-down to enable or disable the URL reclassification facility.

When URL reclassification is enabled a *Submit* button will appear on all blocking pages. Depending on the other URL reclassification settings in this menu, a user may click on the *Submit* button to reclassify the current URL out of the categories under which it has been blocked and may then proceed to view the URL.

ContentKeeper processes *Globally* and *Locally* reclassified URLs in different ways. If *Local URL Reclassification* has been enabled, the user will be presented with two reclassification options after clicking the *Submit* button.

The first option will be to reclassify the URL for the time frame specified for the *Enable Local URL Reclassification* facility. Refer to the Enable Local URL Reclassification section in this chapter for information on how ContentKeeper will process that URL reclassification request.

The second option is to reclassify the URL *Permanently*. This means reclassifying the URL *Globally*. In this case the URL will enter the *Closed Loop Collaborative Filtering*™ process, and will undergo the following steps:

1. ContentKeeper records the category or categories that the URL was blocked under (categories are displayed on the *blockpage*). The URL will then be temporarily suspended from blocking under all categories. At this time the user may proceed to view the URL.

2. Depending on the *Reclassification Server* setting, the URL reclassification request will be submitted to the *ContentKeeper DataCenter* for analysis either directly or via the local ContentKeeper server. Refer to the Reclassification Server section in this chapter for more information.

3. Once analysis has been completed, the new categorisation of the URL is entered into the *ContentKeeper Global URL Database* and collected by the local ContentKeeper appliance on its next hourly database update.

4. The new categorisation of the URL is then entered into the local *Control List* and the temporary suspension of blocking is lifted. The URL will now be blocked in the normal fashion.

Note: Refer to the section ContentKeeper Blocking Explained in Chapter 4 for more information on ContentKeeper blocking.

Enable Local URL Reclassification

Select a time frame from the *Enable Local URL Reclassification* drop-down to enable *Local URL Reclassification*, or select *No* from the *Enable Local URL Reclassification* drop-down to disable *Local URL reclassification*.

ContentKeeper processes *Globally* and *Locally* reclassified URLs in different ways. If *Local URL Reclassification* has been enabled, the user will be presented with two reclassification options after clicking the Submit button.

The first option will be to reclassify the URL for the time frame specified for the *Enable Local URL Reclassification* facility. In this case the URL will undergo the *Local URL Reclassification Steps* outlined below:

The second option is to reclassify the URL *Permanently*. Refer to the Enable URL Reclassification Facility section in this chapter for information on how ContentKeeper will process that URL reclassification request.

Local URL Reclassification Steps

1. ContentKeeper records the category or categories that the URL was blocked under (categories are displayed on the *blockpage*). The URL will then be temporarily suspended from blocking under all categories. At this time the user may proceed to view the URL.

2. Once the time frame specified in the *Enable Local URL Reclassification* setting expires, the temporary suspension of blocking is lifted. The URL will now be blocked in the normal fashion.

Password Protect Above Privileges

Select *Yes* from the *Password Protect Above Privileges* drop-down to force users to enter a password when submitting a URL for reclassification. Passwords are specified under *Reclassification Users*. Refer to the Reclassification Users section in this chapter for more information.

Reclassification Server

This setting allows an administrator specify the server to which *Reclassification Users* will submit URLs for reclassification, *local Server* or *ContentKeeper Base*.

Under most circumstances this should be set to *Local Server*, which will allow the user submitting the URL instant access to it. The URL will then be submitted to the local ContentKeeper appliance via the *Management Port*, which will cause the URL to become unblocked from all categories in the local URL *Control List* (subject to *Closed Loop Collaborative Filtering*™).

Setting the reclassification server to *ContentKeeper Base* will allow the user submitting the URL instant access to it. The URL will then be submitted to the *ContentKeeper DataCenter* via the local network. The URL will then be processed as part of *Closed Loop Collaborative Filtering*™ and distributed

back to the local ContentKeeper appliance where it may become unblocked from the relevant category in the local URL *Control List*.

Setting the reclassification server to *ContentKeeper Base* should only be done when there is no network connectivity between the user-network and the network to which the *Management Port* is attached. This is because there will be no immediate reclassification of the URL in the local *Control List* and there will be no entry made into the reclassified URLs log.

Reclassification Users

Main Menu – Operational Settings → URL Reclassification Settings – Reclassification Users

Use *Reclassification Users* table to specify user names and passwords for those users who you want to have the ability to reclassify URLs when *Password Protect Above Privileges* is enabled.

Local User names may be up to sixteen characters in length.

Local User names may not contain the following characters / \ : ; * ? " < > ~.

ContentKeeper users who can reclassify URLS

Index	UserName	Password	Mode
1	brett	********	Allow
2	john	********	Allow
3	cj	********	Allow
4	michael	**********	Allow
5	mark	********	Allow
6			Allow
7			Allow
8			Allow
9			Allow
10			Allow

Save

The *Reclassification Users* table consists of four columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each username entry for easy reference.
- **UserName** – The *UserName* column accepts username entries, which consist of the user's login name. This is the name that the user will authenticate with.
- **Password** – The *Password* column accepts the password for the username entry in the *UserName* column. This password must also be supplied with the username when authenticating.
- **Mode** – The *Mode* column contains the current mode of the respective username entry. A mode of *Enable* means an authenticating user will be allowed to proceed to the URL reclassification screen if they supply the correct username and password combination. A mode of Dis*able* means an authenticating user will not be allowed to proceed to the URL reclassification screen; regardless of if they supply the correct username and password combination.

Note: The local users database used for *Reclassification Users* is separate from the local users database used for *blockpage* authentication. Entries from one local user database are not automatically available in the other. Refer to the Site/Domain Authentication section in this chapter for more information on user databases for *blockpage* authentication.

Bridge Device Settings

Main Menu – Operational Settings → Bridge Device Settings

Select *Bridge Device Settings* from the *Operational Settings* menu to view and set system device settings and Ethernet device settings for ContentKeeper.

The Device Settings Table

The *Device Settings* table may be found at the top of the *Bridge Device Settings* menu, and contains information about the ContentKeeper *Management Port* and the *Bridge Ports*.

ContentKeeper Bridge Device Settings

Index	Port	Type	IP Address	Driver	Manufacturer
1	eth0	Management	192.9.200.81	eepro100	Intel Corp.|82557/8/9 [Ethernet Pro 100]
2	eth1	Bridge	n/a	eepro100	Intel Corp.|82557/8/9 [Ethernet Pro 100]
3	eth2	Bridge	n/a	eepro100	Intel Corp.|82557/8/9 [Ethernet Pro 100]

The *Device Settings* table consists of six columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each Ethernet port entry for easy reference.
- **Port** – The *Port* column contains the Linux name of an Ethernet interface.
- **Type** – The *Type* column contains a value of either *Management* or *Bridge* and signifies whether the corresponding Ethernet interface in the *Port* column is either a *Management Port* or a *Bridge Port*.
- **IP Address** – The *IP Address* column contains the IP address of the *Management port*. As the *Bridge Ports* do not have IP addresses they have a corresponding value of *n/a* in the *IP Address* column.
- **Driver** – The *Driver* column contains the name of the Linux driver for the Ethernet adaptor relevant to the Ethernet interface specified in the *Port* column.
- **Manufacturer** – The *Manufacturer* column contains the name of the manufacturer of the Linux driver specified in the *Driver* column.

Configuring Ethernet Device Settings

Configuration of the *Management Port* and *Bridge Port* Ethernet device settings is available for supported Ethernet adaptors only, and is achieved via the drop-downs in the *Management Port Settings* table and the *Bridge Port Settings* table.

Note: Refer to the Supported Network Interface Cards section in Chapter 2 for more information on supported Ethernet adaptors.

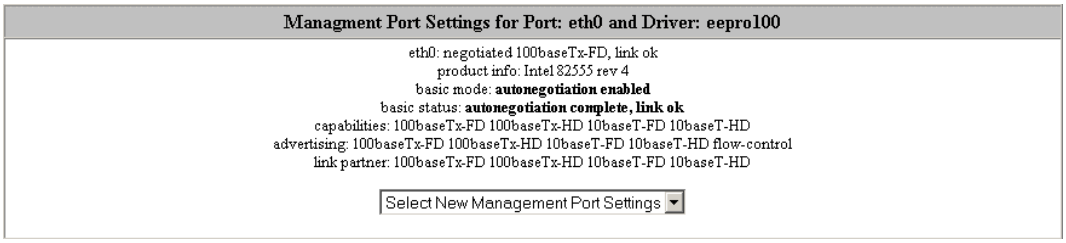
It is possible, via the drop-downs in the *Management Port Settings* table and the *Bridge Port Settings* table, to configure the speed and duplex of the *Management Port* and *Bridge Port* Ethernet adaptors.

Warning: Setting either the *Management Port* and *Bridge Port* Ethernet device settings to a setting that is incompatible with the Ethernet devices that they are connected to will cause them to loose connectivity with the network. In the case of the *Management Port*, this will prevent you from accessing the *ContentKeeper Web Interface*. In the case of the *Bridge Ports*, this will prevent Ethernet traffic from flowing through the *ContentKeeper Bridge*, and may result in a network outage.

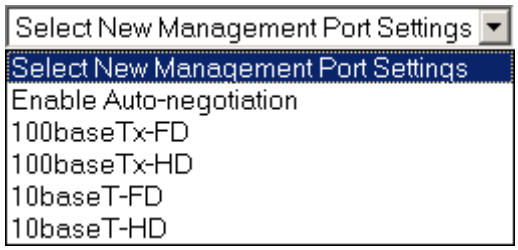
Important! The *ContentKeeper Bridge Ports* must always be set to the same speed and duplex. Also, the devices to which the *Bridge Ports* are connected must always be set to the same speed and duplex.

Management Port Settings Table

Use the *Management Port Settings* table to review and configure Ethernet device settings for the *Management Port*.


Managment Port Settings for Port: eth0 and Driver: eepro100
eth0: negotiated 100baseTx-FD, link ok
product info: Intel 82555 rev 4
basic mode: autonegotiation enabled
basic status: autonegotiation complete, link ok
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
Select New Management Port Settings

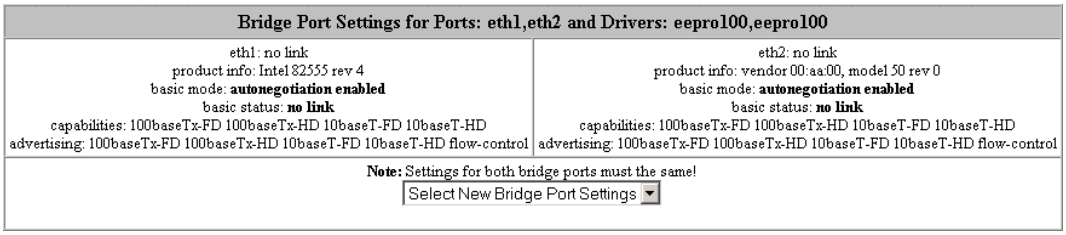
Use the drop-down at the bottom of the *Management Port Settings* table to configure new Ethernet device settings for the *Management Port*.



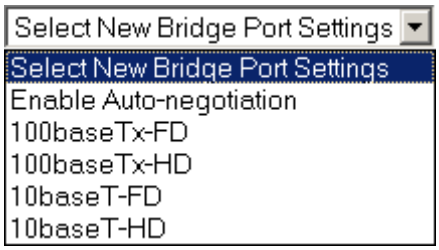
Note: Refer to the Selecting Bridge Device Settings section in this chapter for more information on each of the available device settings.

Bridge Port Settings Table

The *Bridge Port Settings* table to review and configure Ethernet device settings for the *Bridge Ports*.


Bridge Port Settings for Ports: eth1,eth2 and Drivers: eepro100,eepro100
eth1: no link
product info: Intel 82555 rev 4
basic mode: autonegotiation enabled
basic status: no link
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
eth2: no link
product info: vendor 00:aa:00, model 50 rev 0
basic mode: autonegotiation enabled
basic status: no link
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD flow-control
Note: Settings for both bridge ports must the same!
Select New Bridge Port Settings

Use the drop-down at the bottom of the *Bridge Port Settings* table to configure new Ethernet device settings for the *Bridge Ports*.



Note: Refer to the Selecting Bridge Device Settings section in this chapter for more information on each of the available device settings.

Save Redisplay and Execute Button

Click the *Save Redisplay and Execute* button to apply your settings to ContentKeeper.

Refresh Button

After clicking the *Save Redisplay and Execute* button, click the *Refresh* button to view your changes.

Return to Default/Reboot Button

Click the *Return to Default/Reboot* button to force the Ethernet device settings for the *Management Port* and *Bridge Ports* to return to their default state of Auto-negotiate.

Note: This will cause the ContentKeeper appliance to reboot.

Selecting Bridge Device Settings

Use the following information as a guide when selecting new *Management Port* and *Bridge Port* Ethernet device settings.

Enable Auto-negotiation

Selecting this option will cause the *Management Port* and both *Bridge Ports* to automatically attempt to determine the current network bandwidth and duplex.

1000base T/Full

Selecting this option will configure the Ethernet device settings to a network bandwidth of 1000mbps (Gigabit) and to full duplex.

Note: This option is only available when one or more of the installed Ethernet adapters supports Gigabit networking.

100base Tx-Full Duplex

Selecting this option will configure the Ethernet device settings to a network bandwidth of 100mbps and to full duplex.

100base Tx-Half Duplex

Selecting this option will configure the Ethernet device settings to a network bandwidth of 100mbps and to half duplex.

10baseT/UTP-Full Duplex

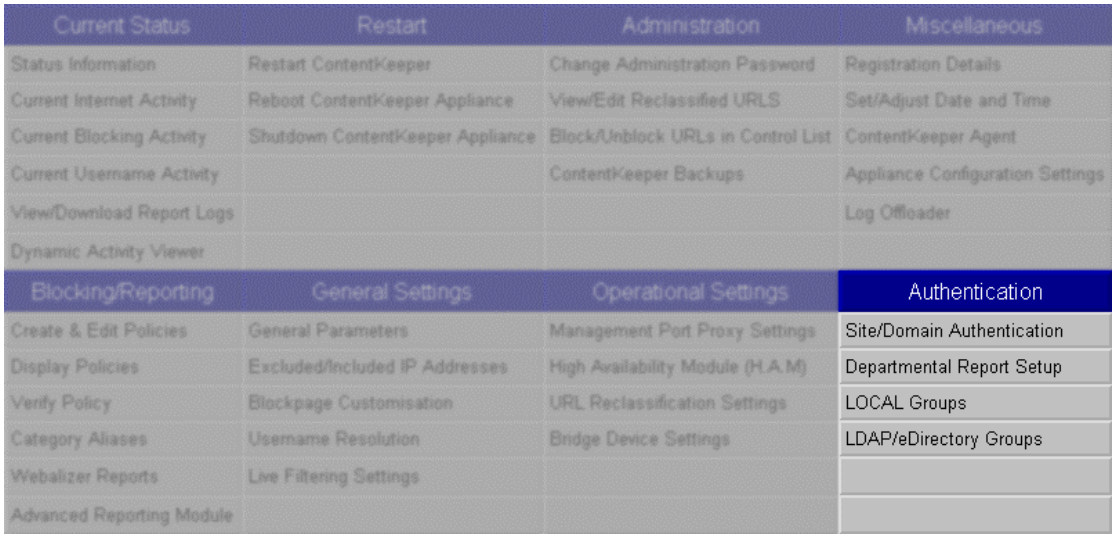
Selecting this option will configure the Ethernet device settings to a network bandwidth of 10mbps and to full duplex.

10baseT/UTP-Half Duplex

Selecting this option will configure the Ethernet device settings to a network bandwidth of 10mbps and to half duplex.

Authentication Menu

The *Authentication* menu contains items that allow you to configure ContentKeeper *Blockpage Authentication*, set up departmental reports and configure *LOCAL* as well as *LDAP/eDirectory Groups* for use with ContentKeeper policies.



Site / Domain Authentication

Main Menu – Authentication → Site/Domain Authentication

The *Site/Domain Authentication* menu allows you to create and manage user accounts for ContentKeeper *blockpage* authentication purposes. Only users with an account defined in the *Site/Domain Authentication* menu will be able to successfully authenticate when blocked by a ContentKeeper *Authenticate blockpage*.

Note: ContentKeeper *blockpage* authentication requires cookies to be enabled on the browser that generates the *Authentication blockpage*. This is usually the user's local browser.

User Database Services

ContentKeeper supports two user database services for the purpose of *blockpage* authentication. These are the ContentKeeper *Local Users* database, and remote *LDAP* databases.

Note: Refer to the State section in this chapter for more information on *Authenticate blockpages* and *blockpage* types.

Note: The local users database used for *blockpage* authentication is separate from the local users database used for policies. Entries from one local user database are not automatically available in the other. Refer to the Select your Directory Services section in this chapter for more information on user databases for policies.

Authenticate Against

Use the *Authenticate Against* drop-down to specify the user database against which users must authenticate when presented with an *Authenticate blockpage*.

Select *Local Users* from the drop-down to force users to authenticate against the *Local Users Database*. The *ContentKeeper Local Users* table only becomes available when *Local Users* is selected from the *Authenticate Against* drop-down, and *Save and Redisplay* is clicked.

Select *LDAP Server* from the drop-down to force users to authenticate against a remote LDAP server. The *ContentKeeper LDAP Server Setup* table only becomes available when *LDAP Server* is selected from the *Authenticate Against* drop-down, and *Save and Redisplay* is clicked.

Click *Save and Redisplay* to apply the settings to ContentKeeper.

Authentication Period

Use the *Authenticate Period* drop-down to specify the period of time for which users will remain authenticated to a site (URL). Once the *Authentication Period* expires, users must re-authenticate. There are 4 options:

- **Browser Session** – When this option is set, a user must authenticate when first challenged by a ContentKeeper *Authenticate* screen. Thereafter, while the browser remains open, the user will not be required to authenticate. Once that browser is closed and a new one opened, the user must start the process again.
- **1 Day** – When this option is set, a user must authenticate when first challenged by a ContentKeeper *Authenticate* screen. After that, the user remains authenticated for 1 day before they must authenticate again.

- **1 Week** – When this option is set, a user must authenticate when first challenged by a ContentKeeper *Authenticate* screen. After that, the user remains authenticated for 1 week before they must authenticate again.
- **1 Month** – When this option is set, a user must authenticate when first challenged by a ContentKeeper *Authenticate* screen. After that, the user remains authenticated for 30 days before they must authenticate again.

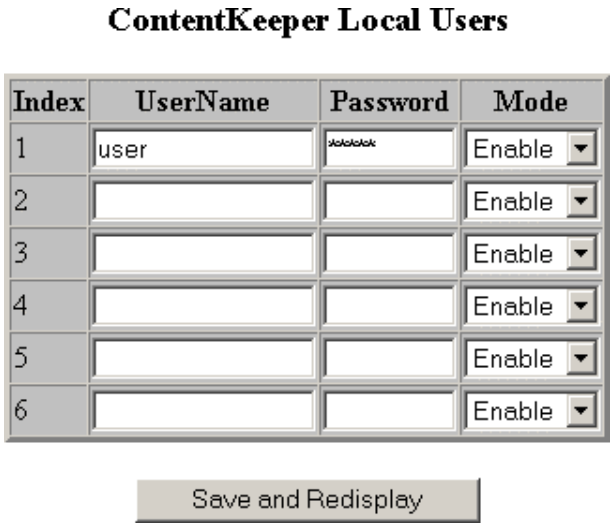
Clear Button

Use this button to clear all authentication tokens and force users to re-authenticate. Usually re-authentication only takes place when a user refreshes the current site within their browser, or attempts to access a link within the current site.

Local Users Database

The *Local Users Database* is stored on the ContentKeeper appliance and may be managed via the *ContentKeeper Local Users* table in the *Site/Domain Authentication* menu. The *ContentKeeper Local Users* table only becomes available when *Local Users* is selected from the *Authenticate Against* drop-down.

Note: Refer to the Authenticate Against section in this chapter for more information on accessing the *ContentKeeper Local Users* table.



The *ContentKeeper Local Users* table consists of four columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each username entry for easy reference.
- **UserName** – The *UserName* column accepts username entries, which consist of the user's login name. This is the name that the user will authenticate with.
- **Password** – The *Password* column accepts the password for the username entry in the previous column. This password must also be supplied with the username when authenticating.
- **Mode** – The *Mode* column contains the current mode of the respective username entry. A mode of *Enable* means an authenticating user will be granted access if they supply the correct username and password combination. A mode of Dis*able* means an authenticating user will not be granted access; regardless of if they supply the correct username and password combination.

The *ContentKeeper Local Users* table is extensible. When all of the available rows are filled and *Save and Redisplay* is clicked, the table will be redrawn with an additional five empty rows.

The *Local Users Database* may contain up to five thousand username entries.

Managing Local Users

Local User names may be up to sixteen characters in length.

Local User names may not contain the following characters / \ : ; * ? " < > ~.

Adding a Local User

To add a user to the *Local Users Database*, enter a username and password into the appropriate columns in the *ContentKeeper Local Users* table, then select a mode and click *Save and Redisplay*.

Removing a Local User

To delete a user from the *Local Users Database*, locate the user in the *ContentKeeper Local Users* table and delete their username and password entries, then click *Save and Redisplay*. Alternatively you may wish to temporarily disable a user. Refer to the Disabling a Local User section for more information.

Disabling a Local User

Disable a user to prevent them from being able to successfully authenticate without removing them from the *Local Users Database*, i.e. prevent the user from accessing *Categories*, *File Types* and *Custom URLs* set to the *Authenticate State.*

To disable a user, select *Disable* from the Mode drop-down in the *ContentKeeper Local Users* table, and then click *Save and Redisplay.*

Remote LDAP Databases

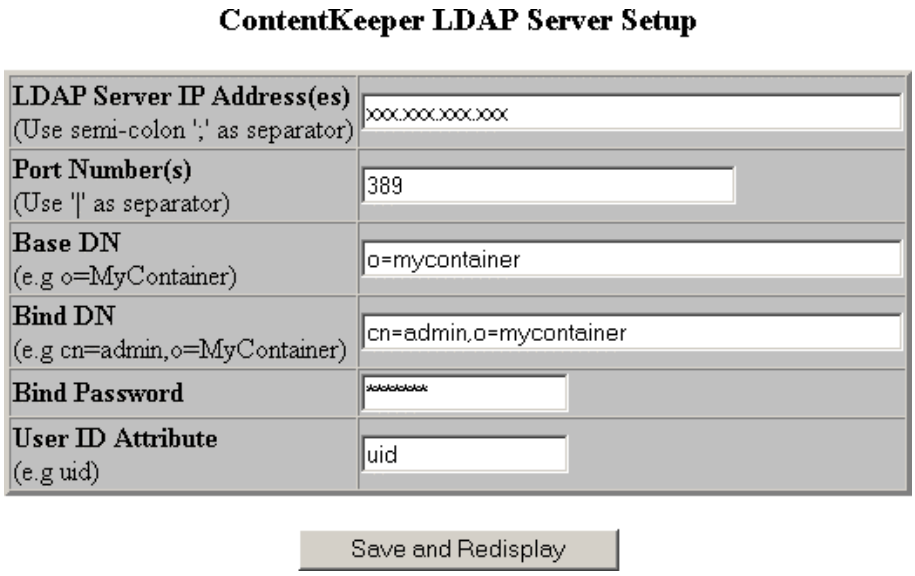
Use the *ContentKeeper LDAP Server Setup* table to configure communications between ContentKeeper and a remote LDAP database. The *ContentKeeper LDAP Server Setup* table only becomes available when *LDAP Server* is selected from the *Authenticate Against* drop-down.

Note: Refer to the Authenticate Against section in this chapter for more information on accessing the *ContentKeeper LDAP Server Setup* table.

ContentKeeper supports *blockpage* authentication against multiple remote LDAP servers.

Note: The *ContentKeeper LDAP Server Setup* used for *blockpage* authentication is separate from the *LDAP/eDirectory Users and Groups Setup* used for policies. Configuring a remote LDAP server for *blockpage* authentication does not automatically configure a remote LDAP server for policies. Refer to the Select your Directory Services section in this chapter for more information on user databases for policies.

Note: Refer to the State section in this chapter for more information on *Authenticate blockpages* and *blockpage* types.



The *ContentKeeper LDAP Server Setup* table consists of a number of server parameter fields, each of which is explained below.

LDAP Server IP Address(es)

Enter the IP address of your LDAP server into the *LDAP Server IP Address(es)* input field in the form of xxx.xxx.xxx.xxx. Do not specify a subnet mask. Multiple IP addresses may be specified if you have multiple LDAP servers, each separated by a semi-colon.

Port Number(s)

Enter the port number into the *Port Number(s)* input field on which ContentKeeper is to connect to the LDAP server. Multiple port numbers may be specified, each separated by a pipe character '|'. The default port number is 389.

Base DN

Enter the base DN (Distinguished Name) into the *Base DN* input field.

Bind DN

Enter the bind DN (Distinguished Name) into the *Bind DN* input field. Multiple container names may be specified, each separated by a comma. The information specified in the *Bind DN* input field will be used by ContentKeeper when authenticating to the LDAP server.

Bind Password

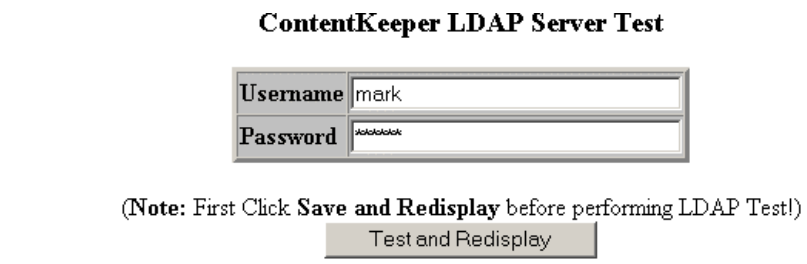
Enter the password used to authenticate and bind to the LDAP directory into the *Bind Password* input field. This information is used by ContentKeeper in conjunction with the information specified in the *Bind DN* input field.

User ID Attribute

Enter the object that you would like the search to return, into the *Filter* input field. This object should contain the users unique username, i.e. the username with which the user authenticates to a proxy server or the LDAP directory with when accessing the Internet. Typically this will be a cn (common name) or a uid (unique identifier).

Testing LDAP Connectivity

Connectivity with the LDAP server may be tested with the test facility below the *ContentKeeper LDAP Server Setup* table. To perform a connectivity test, enter a username and password into the *ContentKeeper LDAP Server Test* table, and then click the *Test and Redisplay* button.


ContentKeeper LDAP Server Test
Username
mark
Password
(Note: First Click Save and Redisplay before performing LDAP Test!)
Test and Redisplay
Please Wait.... Testing LDAP Authentication for Username : mark ....
LDAP Authentication test was successfull!

The test results will be written to the screen when it is redrawn. A successful test will result in a large message in green as seen above; an unsuccessful test will result in a large message in red as seen below.

If the connectivity test fails the reason for the failure may be found in the *LDAP Log Results File*.

Note: Refer to the LDAP Log Results File section in this chapter for more information.

LDAP Log Results File

The *LDAP Log Results File* contains the results of all authentication queries to the LDAP server(s) specified in the *ContentKeeper LDAP Server Setup* table. This includes the results of LDAP server connectivity tests.

To view the *LDAP Log Results File* click on the *Click Here* hyperlink at the bottom of the *Site/Domain Authentication* menu, below the *ContentKeeper LDAP Server Setup* table.

Note: Refer to the Authenticate Against section in this chapter for more information on accessing the *ContentKeeper LDAP Server Setup* table.

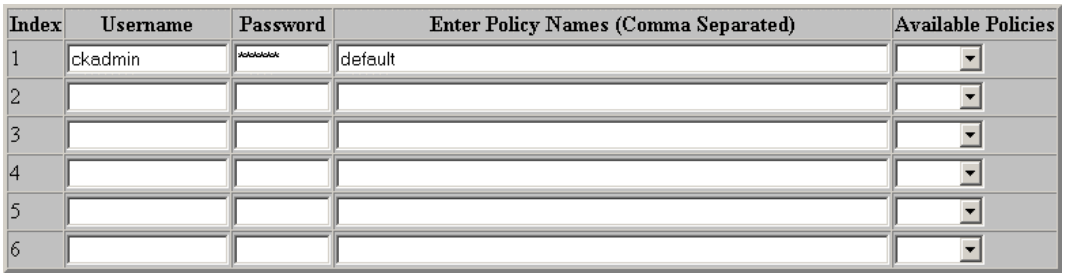
Departmental Reports Setup

Main Menu – Authentication → Departmental Report Setup

ContentKeeper *Departmental Reports* enable authenticated users to view the *Blocking Activity* reports of one or more preselected policies, as well as the global *Webalizer* report, without accessing the main *ContentKeeper Web Interface*.

Managing Departmental Reports User Accounts

Departmental Reports are configured from the *Departmental Report Setup* table. Configuring a *Departmental Report* is achieved by creating a local user account, assigning a password to that account and then specifying which policies *Blocking Activity* reports may be viewed by that account.



Index	Username	Password	Enter Policy Names (Comma Separated)	Available Policies
1	ckadmin	********	default	
2				
3				
4				
5				
6				

The *Departmental Report Setup* table consists of five columns, each of which is defined below:

- **Index** – The *Index* column contains an index of each username entry for easy reference.
- **Username** – The *Username* column accepts username entries, which consist of the user's login name. This is the name that the user will authenticate with when accessing *Departmental Reports*.
- **Password** – The *Password* column contains the password for the username entry in the previous column. This password must also be supplied with the username when authenticating.
- **Enter Policy Names** – The *Enter Policy Names* column accepts a comma-separated list of valid policy names. These are the policies for which *Blocking Activity* reports will be available, within *Departmental Reports*.
- **Available Policies** – The *Available Policies* column consists of a drop-down containing a list of all policy names. Selecting a policy from this drop-down will automatically place that policy name in a comma-separated list in the *Enter Policy Names* column.

The *Departmental Report Setup* table is extensible. When all of the available rows are filled and the *Save* button is clicked, the table will be redrawn with an additional five empty rows.

Departmental Reports user account names may be up to sixteen characters in length.

Departmental Reports user account names may not contain the following characters / \ : ; * ? “ < > ~.

Creating Departmental Reports User Accounts

Use the following procedure to create new *Departmental Reports* user accounts.

1. Click in the next empty *Username* input field and enter a username.

2. Click in the associated *Password* input field and enter a password. The password will be masked for increased security.

3. Use one of the following two methods to populate the *Policy Names* field:

    a. Select a policy from the drop-down in the *Available Policies* column. The policy will then automatically be placed in the *Enter Policy Names* field. Repeat this last step as many times as necessary to add multiple policies to the *Policy Names* field.

    b. Manually type the name of one or more valid policies into the *Enter Policy Names* input field. Each policy name must be separated by a comma with no spaces.

4. Click the *Save* button to apply the changes to the ContentKeeper appliance.

Note: *Departmental Reports* user accounts may be modified using a similar procedure to the above one.

Deleting Departmental Reports User Accounts

To delete a *Departmental Reports* user account, simply delete the desired username entry from the *Username* field along with the associated policies from the *Enter Policy Names* field then click the *Save* button to apply the changes to the ContentKeeper appliance.

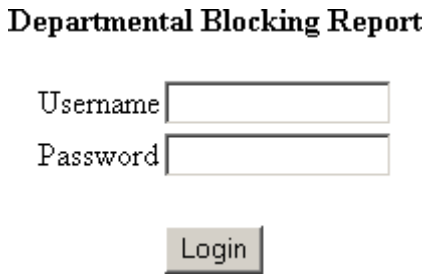
Testing Departmental Reports

Departmental Report accounts may be tested by clicking on the *Click here to Generate and Test Reports* hyperlink at the top of the *Departmental Report Setup* menu, then logging in as the desired user.

Viewing Departmental Reports

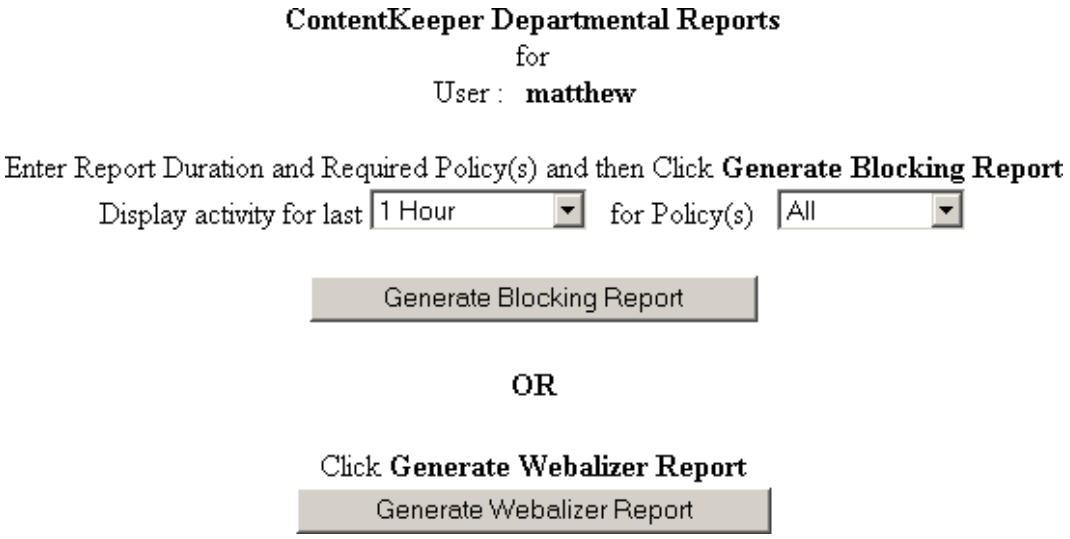
A user with a valid account and password may view a *Departmental Report* by entering the following URL into their browser address bar (where {IPorDNS} represents the IP or DNS address of the local ContentKeeper server):

http://{IPorDNS}/reports.html



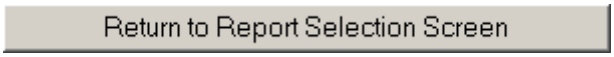
Once the user authenticates they will be presented with a report generation screen from which they may choose to view *Blocking Activity* reports for one or all of the assigned policies. This is achieved by selecting a policy or the term *All* from the drop down box on the right of the screen. The user may also access the global *Webalizer* report from this menu by clicking the *Generate Webalizer Report* button.

Note: Refer to the Webalizer section in this chapter for more information on *Webalizer* reports.



The user must specify the time frame of the report by selecting an option from the *Display activity for last* drop-down on the left side of the screen.

The user may view the report by clicking on the *Generate Blocking Report* button. The user may return to the report generation screen by clicking the *Return to Report Selection Screen* button at the bottom of the report screen.



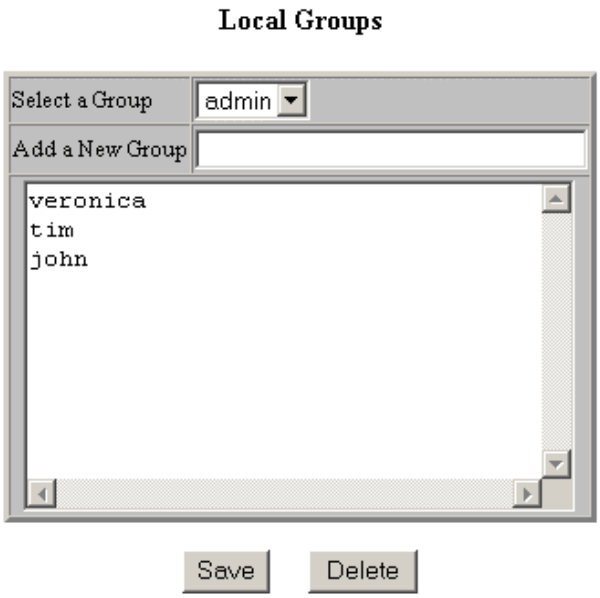
LOCAL Groups

Main Menu – Authentication → LOCAL Groups

Select *LOCAL Groups* from the *Authentication* menu to create and manage local user groups for use in policies. Groups are stored on the ContentKeeper server in the *Local Users Database*.

Note: *LOCAL Groups* are for use with ContentKeeper policies, not for use with *blockpage* authentication. Refer to the Site/Domain Authentication section in this chapter for more information on user databases for *blockpage* authentication.

Note: Refer to the Select your Directory Services section in this chapter for more information on user databases for policies.



Managing LOCAL Groups

LOCAL Group and *LOCAL User* names may be up to thirty-two characters in length. Each *LOCAL Group* may contain up to two thousand users.

LOCAL Group names and *LOCAL User* names may not contain the following characters / \ : ; * ? “ < > ~.

Usernames may be entered one per line or separated by commas. Alternatively you may cut and paste usernames into the username field from another data source. When the *Save* button is clicked, ContentKeeper will organise any entries in the username field in the following manner:

- All upper case letters will be converted to lower case letters.
- All spaces will be removed from group user and names.
- Entries in the username field will be formatted one per line, regardless of the way in which they were entered.
- All duplicate names will be removed.

Creating LOCAL Groups

To create a new *LOCAL Group*, enter a group name into the *Add a New Group* input field then modify the username input field so that it contains the users that you want to belong to this group.

Click the *Save* button to add the new group to the *Local Users Database*.

Modifying LOCAL Groups

To modify the users in a *LOCAL Group*, select the *LOCAL Group* from the *Select a Group* drop-down then make any changes to the username field and click the *Save* button. To modify a *LOCAL Group* name, you must create a new *LOCAL Group*.

Deleting LOCAL Groups

To delete a *LOCAL Group*, select the *LOCAL Group* from the *Select a Group* drop-down menu then click the *Delete* button and confirm your action when prompted.

LDAP/eDirectory Groups

Main Menu – Authentication → LDAP/eDirectory Groups

Select *LDAP/eDirectory Groups* from the *Authentication* menu to configure communications between ContentKeeper and an LDAP or Novell™ eDirectory (NDS) server to allow user and group enumeration for use with ContentKeeper policies.

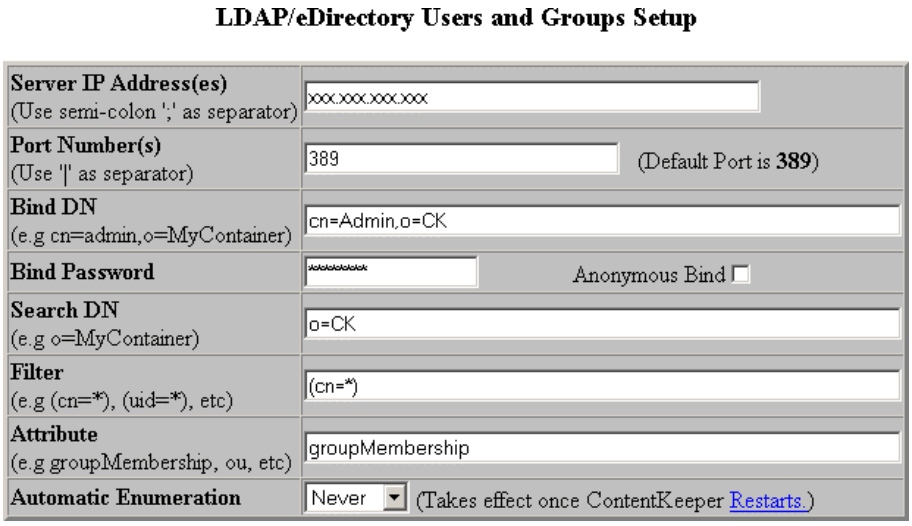
Note: *LDAP/eDirectory Groups* are for use with ContentKeeper policies, not for use with *blockpage* authentication. Configuring a remote LDAP server for policies does not automatically configure a remote LDAP server for *blockpage* authentication. Refer to the Site/Domain Authentication section in this chapter for more information on configuring *blockpage* authentication.

Note: Refer to the Select or Edit your Directory Service section in this chapter for more information on user databases for policies.

LDAP/eDirectory Users and Groups Setup Table

Use the *LDAP/eDirectory Users and Groups Setup* table to configure the settings that ContentKeeper will use to connect to your LDAP server with, as well as to configure how often automatic user and group enumeration will occur.

Click the *Save and Redisplay* button to apply any changes to the ContentKeeper server.



Server IP Address(es)

Enter the IP address of your LDAP server into the *Server IP Address(es)* input field in the form of xxx.xxx.xxx.xxx. Do not specify a subnet mask. Multiple IP addresses may be specified if you have multiple LDAP servers, each separated by a semi-colon.

Port Number(s)

Enter the port number into the *Port Number(s)* input field on which ContentKeeper is to connect to the LDAP server. Multiple port numbers may be specified, each separated by a pipe character '|'. The default port number is 389.

Bind DN

Enter the bind DN (Distinguished Name) into the *Bind DN* input field. Multiple container names may be specified, each separated by a comma. The information specified in the *Bind DN* input field will be used by ContentKeeper when authenticating to the LDAP server.

Bind Password

Enter the password used to authenticate and bind to the LDAP directory into the *Bind Password* input field. This information is used by ContentKeeper in conjunction with the information specified in the *Bind DN* input field.

Anonymous Bind

Check the *Anonymous Bind* check box to force ContentKeeper to bind anonymously to the LDAP directory, instead of using the credentials specified in the *Bind DN* and *Bind Password* fields.

Search DN

Enter the container, or point, in the directory from which to begin the search for your organisations users. Typically this will be an *o* (organisation) or *ou* (organisational unit).

Filter

Enter the object that you would like the search to return, into the *Filter* input field. This object should contain the users unique username, i.e. the username with which the user authenticates to a proxy server or the LDAP directory with when accessing the Internet. Typically this will be a cn (common name) or a uid (unique identifier).

Attribute

Enter the object attribute that is considered to be the group to which the user belongs into the *Attribute* input field. Typically this will be the *groupMembership* attribute or the *ou* (organisational unit) attribute.

If an attribute is not specified, or not found, the *Groupname* for the user becomes the full DN (distinguished name), i.e. that specified in the *Bind DN* field but without the container specified in the *Search DN* field.

Note: You may view example configurations by clicking on the *Click Here for Examples* button at the bottom of the *LDAP/eDirectory Users and Groups Setup* table.

Automatic Enumeration

Users and Groups are enumerated automatically each time ContentKeeper starts or restarts. Use the *Automatic Enumeration* drop-down to specify how often automatic user and group enumeration will occur after ContentKeeper has started. There are four options: *Never*, *Hourly*, *Daily* and *Weekly*.

If *Never* is specified, automatic user and group enumeration will not take place at any time, and ContentKeeper will only enumerate users and groups upon starting or restarting.

Enumerate Now

Click on the *Enumerate Now* button at the bottom of the *LDAP/eDirectory Users and Groups Setup* table to force ContentKeeper to enumerate users and groups from the LDAP server. This feature can be useful for updating the user and group information held by ContentKeeper if you have just made changes to your Directory.

LDAP Log Results File

The *LDAP Log Results File* contains the results of all queries to the LDAP server(s) specified in the *LDAP/eDirectory Users and Groups Setup* table.

To view the *LDAP Log Results File* click on the *Click Here* hyperlink at the bottom of the *LDAP/eDirectory Groups* menu, below the *LDAP/eDirectory Users and Groups Setup* table.

Chapter 6

Reference Section

Chapter 6, the *Reference Section*, will contain information relevant to ContentKeeper but not suitable or too specialised for inclusion in other sections. Chapter 6 consists of the following appendices:

A. Notification of Copyright and License Agreement
B. ContentKeeper Category Definitions
C. Glossary
D. ContentKeeper Technologies Global Office Location
E. High Availability Module Cable Specifications

Appendix A: NOTIFICATION OF COPYRIGHT AND LICENSE AGREEMENT

THIS SOFTWARE PROGRAMME **("Software")** IS A PROPRIETARY PRODUCT OF **CONTENTKEEPER TECHNOLOGIES, A** COMPANY INCORPORATED IN AUSTRALIA.

THE SOFTWARE IS PROTECTED BY COPYRIGHT AND OTHER LAWS. COPYRIGHT LAWS PROHIBIT MAKING AND/OR SELLING ANY ADDITIONAL COPIES OF THE SOFTWARE AND COPYING THE WRITTEN MATERIALS ACCOMPANYING THE SOFTWARE.

SOFTWARE LICENSE AGREEMENT - TERMS AND CONDITIONS

THIS AGREEMENT IS A LEGAL CONTRACT BETWEEN YOU THE **("LICENSEE")** AND **CONTENTKEEPER TECHNOLOGIES** GOVERNING YOUR USE OF THE SOFTWARE. USING THE SOFTWARE INDICATES YOUR UNDERSTANDING AND ACCEPTANCE OF THIS AGREEMENT.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, PROMPTLY RETURN THE COMPLETE SOFTWARE PACKAGE TO THE DEALER FROM WHOM YOU OBTAINED THIS PRODUCT. IN THE CASE OF THE CONTENTKEEPER SOFTWARE BEING DOWNLOADED FROM AN INTERNET WEB SITE, YOU MUST DELETE AND DESTROY ANY COPIES OF THE SOFTWARE DOWNLOADED.

IF YOU HAVE ANY QUESTIONS CONCERNING THIS AGREEMENT, PLEASE CONTACT;

ContentKeeper Technologies
218 Northbourne Avenue
Canberra ACT
Australia 2612
PH +61-2-6261-4950
Fax +61-2-6257-9801
info@ContentKeeper.com
www.ContentKeeper.com

DEFINITIONS

- **CKT.** means ContentKeeper Technologies of 218 Northbourne Ave Braddon ACT Australia 2612 ACN: 079 874 481.
- **Software** means the ContentKeeper software developed solely by CKT.
- **Service** means the provision of the site database and update service, provision of this license to use the CKT Software, and access to the CKT automated software update service.
- **Product** means the Software and the Service and any hardware device (if any) supplied by CKT to Licensee to run the Software.
- **Intellectual Property Rights** means any proprietary right in existence during the term of this agreement including those provided under copyright law, trademark law, patent law, common law, trade secret law or any other statute that may infer any type of ownership and/or rights applicable to the Product including those rights applicable to concepts, inventions, know-how, formulas, ideas, algorithms and methodologies.
- **Domestic Use –** the provision of a filtering service by an Internet Service Provider to domestic residential households **ONLY.**
- **Non Domestic Use** – includes all other use of the Software, including, but not limited to use by an Internet Service Provider and any other individual or organization to provide a filtered service to any person and/or any entity.
- **Evaluation Period** – a once off, maximum period of 20 days from the date the licensee first installs the software on a computer during which time the product may be utilized to determine its suitability for use by that person or organization.
- **Evaluation Licensee** – A licensee who has obtained the software for the sole purpose of evaluating the Software and Service during the Evaluation Period with a view to subscribing to the Service**.**
- **ISP –** Internet Service Provider , an organization in the business of providing Internet access to its customers. An ISP for the purposes of this agreement must have a minimum of 100 domestic household and/or commercial customers to qualify as an ISP.
- **Subscription Period –** The subscription period is a period of 12 months starting from the date the annual Subscription Service Fee is paid to CKT.
- **Due Date** is the date on which the initial Subscription Service Fee is paid by the Licensee to CKT and each subsequent anniversary of that date until this agreement is terminated by either party.
- **Confidential Information –** includes, but is not limited to the terms and conditions of this agreement, the Software, the Site List and the methodologies utilized within the Product.
- **Subscription Service Fee –** is the current annual fee quoted by CKT for use of the Service and is net of any taxes, duties, levies or any other government charges.

1. Grant of License and Provision of Services

License

ContentKeeper Technologies in consideration of the payment made by the Licensee to CKT of the ANNUAL Subscription Service Fee hereby grants to the Licensee a non-exclusive, non-transferable license to use the Software during the Subscription Period ONLY for the purpose of utilizing the CKT service to provide Internet filtering and control services to the number of end users licensed by CKT to receive the Service, in accordance with the terms and conditions outlined in this Agreement.

Payment

Payment of the Subscription Service Fee by the Licensee to CKT on or before the Due Date is of the essence of this agreement. Without prejudice CKT may terminate this agreement if the Licensee fails to pay the full Subscription Service Fee and any other amounts due, on or before the due date. The Licensee also agrees to pay CKT interest at the rate of 18% per annum on any amounts outstanding under this agreement that remain unpaid for any period greater than 45 days and any reasonable costs incurred by CKT in the recovery of any amounts due.

Evaluation

If you have downloaded or otherwise obtained the Software for evaluation ContentKeeper Technologies hereby grants to you, in accordance with the terms and conditions outlined in this Agreement, a non-exclusive, non-transferable license to use the Software on one computer during the **Evaluation Period** only. This grant is limited to one such grant per organization unless prior, express written approval is given to the organization by CKT. At the conclusion of the Evaluation Period you must either delete and/or destroy any copies of the Software obtained or alternatively Subscribe to the Service by paying the Subscription Service Fee to CKT.

Blocking and Control Screens

Licensee hereby agrees to use ContentKeeper's default blocking screen which clearly states that the blocking has been provided by ContentKeeper or if an alternative blocking screen is utilized, that screen must contain the following text in the left hand bottom corner of the blocking screen in bolded courier font of no less that 12 points:-

BLOCKED BY CONTENTKEEPER
WWW.CONTENTKEEPER.COM

General

Licensee may install the Software on as many machines as required to provide filtering services to the number of end users licensed by CKT to receive the Service.

Licensee hereby grants CKT network connectivity access to the Product solely for the purposes of providing the Service (the Service includes bi-directional network traffic to facilitate URL database and Software updates as well as Software and device management services). Licensee hereby agrees to maintain the Software at a version no older than the current released version minus two releases. CKT reserves the right

and the Licensee hereby acknowledges that right to change and or modify the software at any time and without notice to the Licensee.

Licensee hereby grants CKT the right to audit Licensee's use of the software either remotely or on-site to confirm Licensee compliance with this Agreement and Licensee's subscription usage level. This grant also includes any access to Licensees' premises, if requested by CKT, during normal business hours to confirm compliance.

The Licensee's right to use the Software and Services shall cease on the date that the Licensee's Subscription to the CKT Service expires. Upon expiration, the Licensee must delete and destroy any copies of the software and return to CKT at the above address any devices supplied and owned by CKT to Licensee to facilitate the running of the Software, or alternatively secure in writing the express approval of CKT to allow for the destruction of the Software and disposal of any devices supplied and owned by CKT.

2. Copyright Ownership and Confidentiality

(a) The Software contains Confidential Information of ContentKeeper Technologies and all copyright trademarks design rights (registered or unregistered) and other intellectual property rights in the Software, and any translations, modifications, derivatives (whether authorized or unauthorized), are and remain the exclusive property of ContentKeeper Technologies. Intellectual Property Rights includes, without limitation, any rights arising from or capable of arising from the Circuits Layout Act 1989 (Commonwealth); the Copyright Act 1968 (Commonwealth);the Designs Act 1906 (Commonwealth); the Patents Act 1990(Commonwealth); the Trade Marks Act 1995(Commonwealth); any unregistered trade marks or designs; Confidential Information; and any international legislation similar to that legislation listed in this clause.

(b) The Licensee must not:

(i) Make copies of the Software and accompanying written material other than for the purpose of backup and providing the filtering service to the number of users licensed by CKT. Licensee will ensure that such copies bear notice of CKT's ownership of copyright and that the Software contains information confidential to CKT.

(ii) Reverse engineer, decompile, disassemble, or create derivative works based on the Product, the Software, the site lists and/or the service. The Licensee is warned that the Software may include a mechanism which will log such attempts and destroy its operational logic if an attempt is made to tamper with it. ContentKeeper Technologies accepts no responsibility if such a mechanism is activated.

(iii) Rent, lease, sub-license, assign or transfer the Software or any part of it.

(c) The Licensee must not use the Software and its associated Services for any purpose other than to provide the Service to the number of users licensed by CKT to receive the Service.

3. Warranty

(a) ContentKeeper Technologies warrants that it has the rights and title to and owns the property in the Software.

(b) ContentKeeper Technologies give no warranties and makes no representations whatsoever that the Software will be suitable or fit for any particular purpose or for use in any particular networking environment or under any particular conditions notwithstanding that such purpose or condition may be known or have been made known to CKT. CKT gives no warranties that the operation of the Software will not be interrupted or will be error free. The Licensee hereby acknowledges that it has accepted the Software on an "as is" basis and has relied solely on its own investigations to determine the suitability of the software for Licensee's purposes.

(c) Licensee hereby agrees to indemnify CKT, its distributors, resellers and agents against any legal action, initiated by Licensee or any 3rd party for any costs, direct, indirect, consequential, special, collateral, or any other type of losses or damages, loss of profit, loss of data, loss of privacy, loss of access to any sites, losses caused by access to any site, stoppage or impairment of work, loss of goodwill, or loss of network connectivity, or any other losses, costs or expenses relating to the operation of the Product and any related devices within the Licensee's organization and/or networked environment.

(d) The Licensee hereby agrees that under any circumstances whatsoever the total liability of CKT to the Licensee or any 3rd party in respect of the Software and/or Services and any of the provisions of this agreement shall be limited to an amount less than or equal to the annual Subscription Service Fee paid by the Licensee to CKT for the provision of the Software and Services.

(e) CKT makes no representation about the legality of monitoring or using the Product in the Licensee's or any other jurisdiction, and the Licensee hereby declares that it has used its own judgment to verify that the proposed use of the Product complies with any applicable laws, regulations and/or privacy rights.

(f) Licensee hereby acknowledges that Licensee is fully aware that the Software is a filtering application and as such may or may not block and/or operate on particular Internet sites, Internet protocols, traffic and/or files.

(g) Subject to the above, all conditions, warranties, terms and undertakings expressed or implied statutory or otherwise in respect of the Software are hereby excluded, except to the extent that such disclaimers are held to be legally invalid.

Appendix B: ContentKeeper Category Definitions

Introduction

ContentKeepers categories and the ability to block them in various ways form the heart of the product. This being so, it is important to understand what type of web site (URL) goes into each category. ContentKeeper has a total of thirty-two categories, six of which are reserved for future use, and four of which are of special status, i.e. they function differently to the remaining categories (their functionality will be described below).

In the ContentKeeper URL database, a web site may belong to multiple categories. For example, www.discovery.com may belong to the **Entertainment** category and also belong to the **Educational** category. The implications of this are that ContentKeeper may block a web site under more than one category. For more information on web sites blocked under multiple categories and customised web site blocking, refer to the ContentKeeper Administration Guide.

ContentKeeper Technologies has designed the patent-pending **Closed Loop Collaborative Filtering ™** process. As part of the process, any URL submitted for reclassification by a ContentKeeper user will undergo reanalysis at the DataCenter to confirm the accuracy of its present categorisation. This process allows a general users input to act as a fine tuning mechanism, in effect weeding out any incorrectly classified sites. URLs are subsequently redistributed to all ContentKeeper appliances worldwide as part of the hourly URL database update, allowing all users to benefit from the actions of one.

Category 1: **Adult Content**

A web site may be classified under the **Adult Content** category if its content includes the description or depiction of erotic or sexual acts or sexually oriented material such as pornography. Exceptions to this are web sites that contain information relating to sexuality and sexual health, which may be classified under the **Health Sites** Category (21).

Some Example URLs:

- www.playboy.com
- www.worldsex.com
- www.whitehouse.com

Category 2: **News**

A web site may be classified under the **News** category if its content includes information articles on recent events pertaining to topics surrounding a locality (eg. a town, city or nation) or culture, including weather forecasting information. Typically this would include most real-time online news publications and technology or trade journals. This does not include financial quotes, refer to the **Investment Sites** category (11), or sports, refer to the **Sports** category (16). Refer to the section on unique categories at the start of this document.

Some Example URLs:

- www.wsj.com
- www.cnn.com
- www.news.com

Category 3: **Job Search**

A web site may be classified under the **Job Search** category if its content includes facilities to search for or submit online employment applications. This also includes resume writing and posting and interviews, as well as staff recruitment and training services.

Some Example URLs:

- www.spherion.com
- www.monster.com
- www.careerbuilder.com

Category 4: **Gambling**

A web site may be classified under the **Gambling** category if its content includes advertisement or encouragement of, or facilities allowing for the partaking of any form of gambling; For money or otherwise. This includes online gaming, bookmaker odds and lottery web sites. This does not include traditional or computer based games; refer to the **Games Sites** category (10).

Some Example URLs:

- www.casino.com
- www.lottery.com
- www.horse-races.net

Category 5: **Travel / Tourism**

A web site may be classified under the **Travel / Tourism** category if its content includes information relating to travel activities including travelling for recreation and travel reservation facilities.

Some Example URLs:

- www.world-tourism.org
- www.tourism.com.au
- www.deanes.com.au

Category 6: **Shopping**

A web site may be classified under the **Shopping** category if its content includes any form of advertisement of goods or services to be exchanged for money, and may also include the facilities to perform that transaction online. Included in this category are market promotions, catalogue selling and merchandising services.

Some Example URLs:

- www.activeplaza.com
- www.buywineonline.co.uk
- shopping.yahoo.com

Category 7: **Entertainment**

A web site may be classified under the **Entertainment** category if its content includes any general form of entertainment that is not specifically covered by another category. Some examples of this are music sites, movies, hobbies, special interest, and fan clubs. This category also includes personal web pages such as those provided by ISPs. The following categories more specifically cover various entertainment content types, **Pornography / Sex** (1), **Gambling** (4), **Chatrooms** (8), **Game Sites** (10), **Sports** (16), **Clubs and Societies** (22) and **Music Downloads** (23).

Some Example URLs:

- www.britneyspears.com
- www.eonline.com
- www.flydma.com

Category 8: **Chatrooms**

A web site may be classified under the **Chatrooms** category if its content focuses on or includes real-time on-line interactive discussion groups. This also includes bulletin boards, message boards, online forums, discussion groups as well as URLs for downloading chat software.

Some Example URLs:

- www.chatroom.org
- chat.yahoo.com
- web.icq.com/icqchat

Category 9: **Dating Sites**

A web site may be classified under the **Dating Sites** category if its content includes facilities to submit and review personal advertisements, arrange romantic meetings with other people, mail order bride / foreign spouse introductions and escort services.

Some Example URLs:

- adultfriendfinder.com
- www.lavalife.com
- www.singlesites.com

Category 10: **Game Sites**

A web site may be classified under the **Game Sites** category if its content focuses on or includes the review of games, traditional or computer based, or incorporates the facilities for downloading computer game related software, or playing or participating in online games.

Some Example URLs:

- www.ea.com
- gamespot.com
- www.acecheats.com

Category 11: **Investment Sites**

A web site may be classified under the **Investment Sites** category if its content includes information, services or facilities pertaining to personal investment. URLs in this category include contents such as brokerage services, online portfolio setup, money management forums or stock quotes. This category does not include electronic banking facilities; refer to the **E-Banking** category (12).

Some Example URLs:

- www.retireinvest.com.au
- www.stock-options.com
- invest-faq.com

Category 12: **E-Banking**

A web site may be classified under the **E-Banking** category if its content includes electronic banking information or services. This category does not include Investment related content; refer to the **Investment Sites** category (11).

Some Example URLs:

- www.commbank.com.au
- www.natwest.co.uk
- www.cibc.ca

Category 13: **Crime / Terrorism**

A web site may be classified under the **Crime / Terrorism** category if its content includes the description, promotion or instruction in, criminal or terrorist activities, cultures or opinions.

An Example URL:

- www.beatthebandit.com

Category 14: **Personal Beliefs / Cults**

A web site may be classified under the **Personal Beliefs / Cults** category if its content includes the description or depiction of, or instruction in, systems of religious beliefs and practice.

Some Example URLs:

- ccclincolnshire.org
- www.paganfed.demon.co.uk
- www.cultdeadcow.com

Category 15: **Politics**

A web site may be classified under the **Politics** category if its content includes information or opinions of a political nature, electoral information and including political discussion groups.

Some Example URLs:

- www.alp.org.au
- dallas.logcabin.org
- www.politics.com

Category 16: **Sports**

A web site may be classified under the **Sports** category if its content includes information or instructions relating to recreational or professional sports, or reviews on sporting events and sports scores.

Some Example URLs:

- www.sports.com
- www.soccer.com
- www.mtbpics.com.au

Category 17: www-Email Sites

A web site may be classified under the **www-Email Sites** category if its content includes online, web-based email facilities.

Some Example URLs:

- www.hotmail.com
- mail.yahoo.com
- aolmail.aol.com

Category 18: **Violence / Undesirable**

A web site may be classified under the **Violence / Undesirable** category if its contents are extremely violent or horrific in nature. This includes the promotion, description or depiction of violent acts, as well as web sites that have undesirable content and may not be classified elsewhere.

Some Example URLs:

- www.rotten.com
- www.ratemypoo.com

Category 19: **Malicious**

A web site may be classified under the **Malicious** category if its content is capable of causing damage to a computer or computer environment, including the unauthorised consumption of network bandwidth.

An Example URL:

- astalavista.box.sk

Category 20: **Search Sites**

A web site may be classified under the **Search Sites** category if its main focus is providing online Internet search facilities. Refer to the section on unique categories at the start of this document.

Some Example URLs:

- www.google.com
- www.yahoo.com
- www.altavista.com

Category 21: **Health Sites**

A web site may be classified under the **Health Sites** category if its content includes health related information or services, including sexuality and sexual health, as well as support groups, hospital and surgical information and medical journals.

Some Example URLs:

- www.samhsa.gov
- www.personalhealthzone.com
- www.safemedication.com

Category 22: **Clubs and Societies**

A web site may be classified under the **Clubs and Societies** category if its content includes information or services of relating to a club or society. This includes team or conference web sites.

Some Example URLs:

- www.apex.com
- www.sierraclub.org
- www.isoc.org

Category 23: **Music Downloads**

A web site may be classified under the **Music Downloads** category if it provides online music downloading, uploading and sharing facilities as well as high bandwidth audio streaming.

Some Example URLs:

- www.musicmass.com
- www.mp3.com
- www.mp3dimension.com

Category 24: **Business Oriented**

A web site may be classified under the **Business Oriented** category if its content is relevant to general day-to-day business or proper functioning of the Internet, eg. Web browser updates. Access to web sites in this category would in most cases not be considered unproductive or inappropriate. Refer to the section on unique categories at the start of this document.

Category 25: **Government Blocking List**

This category is populated by URLs specified a government agency, and contains URLs that are deemed unsuitable for viewing by the general public by way of their very extreme nature.

Some Examples are:

- Child pornography sites
- Beastiality sites
- Rape sites

Category 26: **Educational**

A web site classified under the **Educational** category may belong to other categories but has content that relates to educational services or has been deemed of educational value, or to be an educational resource, by educational organisations. This category is populated by request or submission from various educational organisations. Refer to the section on unique categories at the start of this document.

Some Example URLs:

- www.discovery.com
- highschoolhub.org
- www.home-school.com

Category 27: **Advertising**

A web site may be classified under the **Advertising** category if its main focus includes providing advertising related information or services.

Some Example URLs:

- www.traffimagic.com
- www.ads.com
- www.doubleclick.com

Category 28: **Drugs/Alcohol**

A web site may be classified under the **Drugs/Alcohol** category if its content includes drug and alcohol related information or services. Some URLs categorised under this category may also be categorised under the Health category.

Some Example URLs:

- www.online-cocktail-guide.com
- www.jackdaniels.com
- www.cultdrinks.com

Category 29: **Computing/IT**

A web site may be classified under the *Computing/IT* category if its content includes computing related information or services.

Some Example URLs:

- www.redhat.com
- www.squid-cache.org
- www.gnu.org

Category 30: **Swimsuit/Lingerie/Models**

A web site may be categorised under the Swimsuit/Lingerie/Models category if its content includes information pertaining to, or images of swimsuit, lingerie or general fashion models.

Some Example URLs:

- ralph.ninemsn.com.au
- www.victoriassecret.com
- sportsillustrated.cnn.com/features/2002/swimsuit

Appendix C: Glossary

Adaptive Ethernet Bridge – An adaptive Ethernet bridge is a device that passes data packets between multiple network segments that use the same communication protocols. An adaptive bridge passes one signal at a time. If a packet is destined for a computer within the senders own network segment, the adaptive bridge retains the packet within that segment. If a packet is destined for a segment different from the one where it originated then the bridge will forward the packet.

BOOTP – An acronym for **Boot**strap **P**rotocol. BOOTP uses IP or UDP Protocols. It allows a client machine to discover its own IP address, the address of a server host, and the name of a file to be loaded into memory and executed. The bootstrap operation can be thought of as consisting of two phases. The first phase, which could be labelled 'address determination and boot file selection'. After this address and filename information is obtained, control passes to the second phase of the bootstrap where a file transfer occurs. The file transfer will typically use the TFTP protocol, since it is intended that both phases reside in ROM on the client. However BOOTP could also work with other protocols such as SFTP or FTP.

Bridge – Refer to *Adaptive Ethernet Bridge*.

Buffer – A region of RAM reserved for use with data that is temporarily held while waiting to be transferred between two locations, such as between an application’s data area and an input / output device.

Cache – A small, fast portion of memory holding recently accessed data, designed to speed up subsequent access to the same data. Most often applied to processor-memory access but also used for a local copy of data accessible over a network etc.

Caching Proxy Server – A server that sits between a client application, such as a Web browser, and an actual server. When a caching proxy server receives a request for a URL, it looks for the URL in its local cache. If found, it returns the document immediately, otherwise it retrieves it from the remote server, saves a copy in the cache and returns it to the requester. The cache will usually have an expiry algorithm, which flushes documents according to their age, size, and access history.

Control List – A list containing categorised URLs. In the content filtering process any URL that is browsed to is compared to this list and, if there is a match then the URL is processed in a predefined way. If there is not a match then the URL is not processed.

Control List Blocking – This refers to the process of blocking URLs based on entries in the local Control List. Refer to *Control List*.

DMZ – A **D**e-**M**ilitarised **Z**one, or Secure Server Network (SSN). A DMZ is used by an organisation that wants to host Internet services without allowing unauthorized access to its private network. The DMZ sits between the Internet and an internal network's line of defence, usually a firewall. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Ethernet – Ethernet is a popular LAN technology that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) between clients over a variety of cable types. Ethernet is passive which means that it requires no power source of it's own, and thus does not fail unless the cable is physically cut or improperly terminated. Ethernet uses multiple communication protocols and can connect mixed computing environments, including NetWare, UNIX, Windows and Macintosh.

Firewall – A dedicated gateway server configured with special security criteria. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All traffic entering or leaving the intranet passes through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

Globally Reclassified URLs – URLs that have been reclassified and uploaded into the ContentKeeper Technologies Data Centre Database and subsequently made available to all ContentKeeper Clients worldwide.

High Availability Module – An electro-mechanical device that monitors the ContentKeeper Appliance to ensure Ethernet connectivity. The H.A.M. is configured to watch for a polling signal from the ContentKeeper Appliance at a predefined interval. Should this signal fail to be transmitted (an indication that the ContentKeeper Appliance has stopped), mechanical relays inside the H.A.M. will close and short circuit the ContentKeeper Adaptive Ethernet Bridge, effectively cutting the ContentKeeper Appliance out of the Ethernet circuit and allowing continued (unfiltered) Internet access.

Host – Refer to *Node*.

Hub – Hubs are connectivity devices that connect computers in a star topology. Hubs contain multiple ports for connecting to network components. If you use a hub, a break in the network does not affect the entire network; only the segment and the computer attached to that segment fail. A single data packet sent through a hub is transmitted to all ports on the hub.

ICMP - **I**nternet **C**ontrol **M**essage **P**rotocol. An extension to the Internet Protocol (IP) that allows for the generation of error messages, test packets, and informational messages related to IP. It is defined in STD 5, RFC 792.

Live Blocking – ContentKeeper will classify previously unexplored URLs immediately, as they are browsed to. If a newly classified URL is classified under a category that you have configured to block then any further attempts to browse to that URL will be blocked. Any newly classified URLs are uploaded into the ContentKeeper Technologies Data Centre Database and made available globally. Refer to *Globally Reclassified URLs*.

Locally Reclassified URLs – URLs that have been reclassified within the local Control List. These are only available to local clients. Refer to *Control List*.

Memory – Random Access Memory (RAM). Refer to *RAM*.

Node – An addressable device attached to a computer network, more often called a "host". A node can be a computer or some other device, such as a printer. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address.

PING – It is often believed that PING is an abbreviation for ***P****acket* ***In****ternet* ***G****roper,* but Ping's author has stated that the name was originally contrived to match submariners' term for the sound of a returned sonar pulse. PING is a utility used to test connectivity to destination hosts by sending them one, or repeated, ICMP (Internet Control Message Protocol) echo requests and waiting for and displaying any replies. In its most basic form, a PING command may be issued as *ping 192.9.200.32*, where *192.9.200.32* is the IP address of the desired host.

Port – A logical channel or channel endpoint in a communications system. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) used on Ethernet use port numbers to distinguish between (de-multiplex) different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it, defined in /etc/services or the Network Information Services "services" database. Some protocols, e.g. telnet and HTTP have default ports but can use other ports as well. Refer to *Ethernet*.

Promiscuous Mode – A mode of operation associated with Ethernet cards, where a card accepts all packets, regardless of their destination address, as opposed to normal operation where a card will only accept packets destined for it.

Proxy – Refer to *Caching Proxy Server*.

RAM – **R**andom **A**ccess **M**emory. A data storage device for which the order of access to different locations does not affect the speed of access. This is in contrast to, say, a hard disk or magnetic tape where it is very much quicker to access data sequentially because accessing a non-sequential location requires physical movement of the storage medium rather than just electronic switching. RAM is also known as volatile memory as any data stored in it is lost when power is turned off.

Router – A router is a device that acts like a bridge or a switch but provides more functionality. In moving data between different network segments, routers examine a packet header to determine the best path for the packet to travel. A router knows the path to all of the segments on the network by accessing information stored in a routing table. Routers enable all users in a network to share a single connection to the Internet or a WAN. Refer to Bridge and Switch.

SSN – Refer to DMZ.

Switch – Switches are similar to bridges but offer a more direct connection between the source and destination computers. When a switch receives a data packet, it creates a separate internal connection, or segment, between any two of it's ports and forwards the data packet to the appropriate port of the destination computer only, based on information in the data packets header. This insulates the connection from other ports and gives the source and destination computers access to the full bandwidth of a network. Refer to Bridge.

URL – **U**niversal **R**esource **L**ocater. Also known as an Internet address.

VLAN – **V**irtual **L**ocal **A**rea **N**etwork. A logical grouping of two or more nodes which are not necessarily on the same physical network segment but which share the same IP network number. Computers connected to a VLAN behave as if they are connected to the same wire even though they may actually be in different physical locations.

WatchDog – Refer to *High Availability Module*.

Appendix D: ContentKeeper Technologies Global Office Location

Asia Pacific (Head Office)

Mail: ContentKeeper Technologies
218 Northbourne Avenue
Braddon ACT 2612
Australia

Phone: +61 2 62614950

Fax: +61 2 62579801

Email: support@contentkeeper.com

Europe

Mail: ContentKeeper Technologies Europe
PO Box 7868
Crowthorne
RG45 6XY
United Kingdom

Phone: +44 0 1344 752740

Fax: +44 0 1344 780332

Email: support@contentkeeper.co.uk

Americas

See ContentKeeper Technologies Asia/Pacific or Europe offices for contact details.

Appendix E: High Availability Module Cable Specifications

Internal Interface Cable Specifications

To use an internal interface cable the ContentKeeper server's server board must have an internal 10-pin serial header. Refer to the server board documentation for more information. Use the following table as a guide when constructing a cable.

Important: Ensure that the cable is long enough to reach from the 10-pin header on the server board to the female DB9 socket on the H.A.M.

Specifications: 10-pin socket to Male DB9 plug

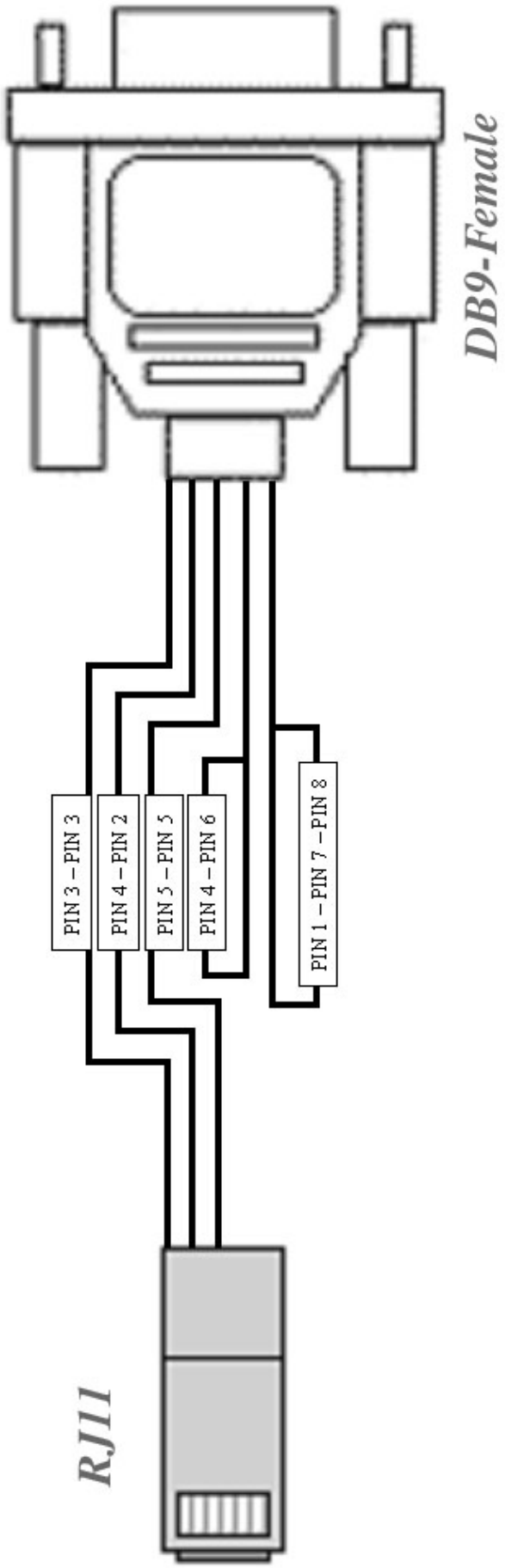
Header Pin No.	DB9 Male Pin No.
1	1
2	6
3	2
4	7
5	3
6	8
7	4
8	9
9	5
10	-

External Interface Cable Specifications

Use the following figures as a guide when constructing a cable. Note that pins 4 and 6 on the DB9 socket should be soldered together and that pins 1, 7 and 8 on the DB9 socket should also be soldered together.

To determine Pin-1 on an RJ11 connector, look into the RJ11 Socket with the key on the bottom, Pin-1 is on your left. Use the following table as a guide when determining the pin order on an RJ11 connector.

RJ11 Pin	Wire Colour
1	Blue
2	Yellow
3	Green
4	Red
5	Black
6	White


DB9-Female
PIN 3 – PIN 3
PIN 4 – PIN 2
PIN 5 – PIN 5
PIN 4 – PIN 6
PIN 1 – PIN 7 – PIN 8
RJ11

Index

A

Administering ContentKeeper
  Administration Life Cycle, 75
  Blocking Fundamentals, 83
    Blocking States, 87
    Blocking Types, 83
  Overview, 74
Administration Life Cycle, 75
Administration Menu, 141
  Block / Unblock URLs In Control List, 144
  Change Administration Password, 142
  ContentKeeper Backups, 148
  View / Edit Reclassified URLS, 142
Advanced Reporting Module Menu, 201
Appendix A: NOTIFICATION OF COPYRIGHT AND LICENSE AGREEMENT, 258
Appendix B: ContentKeeper Category Definitions, 263
Appendix C: Glossary, 274
Appendix D: ContentKeeper Technologies Global Office Location, 278
Appendix E: High Availability Module Cable Specifications, 279
Appliance. *See* ContentKeeper Appliance
Appliance Configuration Settings Menu, 162
Authentication Menu, 241
  Departmental Reports Setup, 248
  LDAP/eDirectory Groups, 253
  LOCAL Groups, 251
  Site / Domain Authentication, 241
Auto Installer, 50

B

Block / Unblock URLs In Control List Menu, 144
  Reclassification History, 148
Blocking / Reporting Menu, 167
  Advanced Reporting Module, 201
  Category Aliases, 190
  Create & Edit Policies. *See* Policies
  Display Policies, 185
  Verify Policy Menu, 187
  Webalizer Reports, 190
Blockpage Customisation Menu, 207
  Configuring
    Authenticate Blockpage, 208
    Customised Blockpages, 207
    Enabling, 207
  Example Code, 208

Bridge Device Settings Menu, 236
  Configuring
    Ethernet Device Settings, 237
Bridge Ports
  Cabling, 65
  Configuring Bridge Device Settings, 99
  Example Deployment Scenarios, 65
  Network Location, 64
  Viewing Port Status, 127
  Viewing Traffic Statuc, 128
Building a ContentKeeper Appliance
  BIOS Setup, 40
  Bridge Ports. *See* Bridge Ports
  ContentKeeper Setup Program, 51
    Accessing from the Console Screen, 54
    Accessing from the Remote Serial Console, 54
  Ethernet Device Order, 39
  Hardware Setup, 39
  Installing ContentKeeper, 50
  Management Port. *See* Management Port
  Obtaining Configuration Information, 34
  Operating System, 33
  Supported Network Interface Cards, 33
  System Requirements, 32
  Using the ContentKeeper Auto Installer, 50

C

Category Aliases Menu, 190
Category Definitions, 263
  Adult Content, 264
  Advertising, 272
  Business Oriented, 271
  Chatrooms, 266
  Clubs and Societies, 271
  Computing/IT, 273
  Crime / Terrorism, 268
  Dating Sites, 266
  Drugs/Alcohol, 273
  E-Banking, 267
  Educational, 272
  Entertainment, 266
  Gambling, 265
  Game Sites, 267
  Government Blocking List, 272
  Health Sites, 270
  Investment Sites, 267
  Job Search, 264
  Malicious, 270
  Music Downloads, 271
  News, 264

Personal Beliefs / Cults, 268
Politics, 268
Search Sites, 270
Shopping, 265
Sports, 269
Swimsuit/Lingerie/Models, 273
Travel / Tourism, 265
Violence / Undesirable, 269
www-Email Sites, 269
Change Administration Password Menu, 142
Chapter 1: QuickStart Guide, 17
Chapter 2: Building a ContentKeeper Appliance, 27
Chapter 3: Deploying ContentKeeper, 59
Chapter 4: Administering ContentKeeper, 73
Chapter 5: Configuring ContentKeeper, 124
Chapter 6: Reference Section, 257
Cisco WCCP-GRE Support, 64
Closed Loop Collaborative Filtering, 82
Configuration Information. *See* Obtaining Configuration Information
ContentKeeper Agent, 154
Accessing the Agent Monitor, 159
Configuring
ContentKeeper, 155
The Agent, 158
Installing, 156
Log File, 160
Software Updates, 161
Stopping And Restarting, 159
ContentKeeper Appliance, 28
ContentKeeper LE Appliance, 30
ContentKeeper SME Appliance, 29
ContentKeeper Backups Menu, 148
Default Setup, 151
Performing, 150
Recommended Backup Regime, 113
Restoring Backups, 151
ContentKeeper Bridge Ports. *See* Bridge Ports
ContentKeeper Filtering Explained, 78
ContentKeeper Management Port. *See* Management Port
ContentKeeper Reporting, 114
ContentKeeper Setup Program. *See* Building a ContentKeeper Appliance
Context Sensitive Help, 12
Create & Edit Policies Menu. *See* Policies
Current Blocking Activity Menu, 130
Current Internet Activity Menu, 129
Current Status Menu, 125
Current Blocking Activity, 130
Current Internet Activity, 129
Current Username Activity, 132
Dynamic Activity Viewer, 137

Status Information, 125
View / Download Report Logs, 134
Current Username Activity Menu, 132
Custom URLs
Configuring, 181
Custom IP Addresses, 182
Custom URL Entry Rules, 183
Mode of Operation, 86, 181

D

DataCenter Connectivity
Deployment Planning Guidelines, 67
Viewing Connectivity Status, 129
Date. *See* Set / Adjust Date and Time Menu
Departmental Reports Setup Menu, 248
Managing Departmental Reports User Accounts, 248
Creating, 249
Deleting, 249
Testing, 250
Deploying ContentKeeper
Deploying ContentKeeper, 68
Deployment Guidelines, 68
Initial ContentKeeper Configuration, 69
Planning to Deploy ContentKeeper, 61
Deployment Planning Guidelines, 61
Filtering of Local Network Segments, 62
Filtering of Remote Network Segments, 62
Filtering Proxy Server Traffic, 63
Management Port. *See* Management Port
Display Policies Menu, 185
Current List of Policies Table, 186
Other Rules / Policies Table, 186
Document Conventions, 13
Document Layout, 14
Dynamic Activity Viewer Menu, 137

E

eDirectory. *See* LDAP/eDirectory Groups
Evaluation Software, 12
Excluded / Included IP Addresses Menu, 204
Configuring
Catch All Mode, 205
Configuration Guidelines, 98
Examples, 206
IP Address Table, 204

F

File-Types
Configuring, 179

Filtering Explained, 78
Blocking Fundamentals, 83
Blocking States, 87
Blocking Types, 83
Closed Loop Collaborative Filtering, 82
Live Filtering, 83
Overview, 78
Policy Logic And Implementation Requirements, 79

G

General Parameters Menu, 202
Configuration Guidelines, 100
ContentKeeper Blocking, 203
Live Filtering Settings, 222
Port Numbers For Filtering, 203
General Settings Menu, 202
Blockpage Customisation, 207
Excluded / Included IP Addresses, 204
General Parameters, 202
Username Resolution, 210
Getting the most out of this guide, 13

H

High Availability Module (H.A.M)
Cause Codes and Uptime, 231
ContentKeeper Setup, 228
Configuration Overview, 228
ContentKeeper Configuration Procedures, 231
Hardware Setup, 43
Connecting the Internet and Enterprise LAN ports, 48
Identifying Ports, 47
Installing, 43
Introduction to, 42
Viewing Status, 126

I

Initial ContentKeeper Configuration, 69
Installing ContentKeeper. *See* Building a ContentKeeper Appliance
Introduction, 11
Introduction to ContentKeeper, 14

L

LDAP/eDirectory Groups Menu, 253
Configuring, 253
LDAP Log Results File, 256
Live Filtering Explained, 83
Live Filtering Settings Menu, 222
Configuring
Live Filtering Aggressiveness, 222

Live Filtering Language Settings, 223
Local Groups Menu, 251
Managing LOCAL Groups, 252
Creating, 252
Deleting, 253
Modifying, 253
Log Offloader Menu, 163
Configuring, 163
The Log Table, 164
View Status Log, 166

M

Management Port
Configuring
Configuring with the ContentKeeper Setup Program, 51
Connecting to a Network, 53
Proxy Server Bypass, 98
Deployment Planning Guidelines
Connectivity With Network Clients, 68
DataCenter Connectivity, 67
Network Location, 67
Username Resolution, 68
Management Port Proxy Settings Menu, 225
Configuring
Authentication Settings, 226
Proxy Server Settings, 225
Testing Connectivity, 227
Miscellaneous Menu, 152
Appliance Configuration Settings, 162
ContentKeeper Agent, 154
Log Offloader, 163
Registration Details, 152
Set / Adjust Date and Time, 153

N

NT Agent. *See* ContentKeeper Agent

O

Obtaining Configuration Information, 34
Obtaining Evaluation Software, 12
Obtaining Technical Support, 12
Operational Settings Menu, 225
Bridge Device Settings, 236
Management Port Proxy Settings, 225
URL Reclassification Settings, 232

P

Personal Surfing Units, 89
Configuring, 174

Blocking States, 175
Control Period, 174
Global Parameters, 175
Resetting P.S.U Controls, 179
Viewing
Control Status, 176
P.S.U Usage Details, 177
Planning to Deploy ContentKeeper, 61
Policies
Configuring, 169
Categories, 169
Cloning Guidelines, 104
Cloning Policies, 169
Configuration Guidelines, 103
Create & Edit Policies Menu, 168
Custom URLs. *See* Custom URLs
Directory Objects, 107
Directory Services, 106
File-Types. *See* File-Types
Other Rules, 184
P.S.U Settings. *See* Personal Surfing Units, Configuring
Policy Blocking Rules, 105
Time Of Day Settings. *See* Time of Day, Configuring
Default Only Mode, 168
Default Policy Defined, 110
Enabling, 110
Global Policy Defined, 110
Overview, 102
Policy Logic And Implementation Requirements, 79
Silent Mode, 111
Verifying, 109
Policy Logic And Implementation Requirements, 79
Proxy Servers
Configuring Management Port for, 225
Deployment Planning Guidelines, 63
Excluding / Bypassing, 204

R

Reboot ContentKeeper Appliance Menu, 140
Rebuilding a ContentKeeper Appliance, 121
Reclassification History, 148
Reclassification Users, 235
Registration Details Menu, 152
Remote Serial Console, 55
Report Log Settings, 136
Restart ContentKeeper Menu, 140
Restart Menu, 139
Reboot ContentKeeper Appliance, 140
Restart ContentKeeper, 140
Shutdown ContentKeeper Appliance, 141

S

Set / Adjust Date and Time Menu, 153
Setup Program. *See* Building a ContentKeeper Appliance, ContentKeeper Setup Program
Shutdown ContentKeeper Appliance Menu, 141
Silent Mode, 111
Site / Domain Authentication Menu, 241
  Configuring
    Authentication Period, 242
    Local Users Database, 243
    Remote LDAP Databases, 245
    User Database Services, 241
Status Information Menu, 125

T

Technical Support, 12
Time. *See* Set / Adjust Date and Time Menu
Time of Day
  Accessing, 171
  Configuring, 172
  Example Configuration, 173
Troubleshooting, 115
  Troubleshooting DataCenter Connectivity, 115
  Troubleshooting the H.A.M, 118, 120
Tuning ContentKeeper Configuration, 92

U

URL Reclassification Settings Menu, 232
  Configuring
    Global URL Reclassification, 232
    Local URL Reclassification, 233
    Reclassification Users, 235
Username Resolution Menu, 210
  Configuring
    IP Address Mode, 211
      eDirectory Settings, 215
    None Mode, 210
    ProxyHeader Mode, 216
  Testing, 219

V

Verify Policy Menu, 187
  Realtime Verification, 188
  Verify Input on All Policies, 188
  Verify Input on Single Policy, 188
View / Download Report Logs Menu, 134
  Report Log Settings, 136
View / Edit Reclassified URLS Menu, 142
  Global Reclassified URLS, 142

Local URL Reclassifications, 143

W

WCCP Support. *See* Cisco WCCP-GRE Support
Webalizer Reports Menu, 190
Report Types and Totals, 192
Who should use this guide, 13